Bacheloroppgave

NTNU
Norges teknisk-naturvitenskapelige universitet
Fakultet for informasjonsteknologi og elektroteknikk
Institutt for datateknologi og informatikk

Erling Cockerell Fladvad
Fabian Hauge Sandvik
Jørgen Torset Nilsen

NSMs grunnprinsipper i praksis

En kvalitativ studie av sikkerhetskopieringspraksiser hos SMB

Bacheloroppgave i Digital infrastruktur og cybersikkerhet
Veileder: Olav Skundeberg

Mai 2023

NTNU
Kunnskap for en bedre verden

Erling Cockerell Fladvad
Fabian Hauge Sandvik
Jørgen Torset Nilsen

NSMs grunnprinsipper i praksis

En kvalitativ studie av sikkerhetskopieringspraksiser hos SMB

Bacheloroppgave i Digital infrastruktur og cybersikkerhet
Veileder: Olav Skundeberg
Mai 2023

Norges teknisk-naturvitenskapelige universitet
Fakultet for informasjonsteknologi og elektroteknikk
Institutt for datateknologi og informatikk

NTNU
Kunnskap for en bedre verden

Sammendrag

Formålet med *NSMs grunnprinsipper i praksis* er å bidra til å redusere små og mellomstore bedrifter (SMB) sin sårbarhet til IKT-sikkerhetshendelser.

IKT-sikkerhetsarbeid kan være utfordrende for SMB som ofte har mindre ressurser og kompetanse enn større bedrifter. Nasjonalt cybersikkerhetssenter erfarer at dersom virksomheter i større grad hadde implementert NSMs grunnprinsipper for IKT-sikkerhet, så kunne alle hendelser vært unngått eller skaden begrenset. For å bidra til å redusere SMB sin sårbarhet til IKT-sikkerhetshendelser, vil vi derfor undersøke hvordan etterlevelsen av NSMs grunnprinsipper for IKT-sikkerhet kan økes.

Gjennom dybdeintervjuer med 11 ansatte med ansvar for IKT-sikkerhet i hver sine respektive SMB, undersøker vi hvilket forhold de har til NSMs grunnprinsipper for IKT-sikkerhet og måler til hvilken grad prinsippene etterleves. Vi ser også på forhold som påvirker etterlevelsen og hvilke utfordringer bedriftene har med IKT-sikkerhetsarbeid. I etterkant av intervjuene følger vi opp informantene med en spørreundersøkelse.

Det kommer frem at bedriftenes rutiner og prosesser for sikkerhetskopiering samsvarer med NSMs anbefalinger i lav til middels grad. Dette antyder at det er behov for å øke etterlevelsen av NSMs grunnprinsipper og det kan se ut til at informantene også så et behov for det. Vi erfarte at det som hadde størst påvirkning på informantene var bevisstgjøringen som følge av intervjuene. I etterkant av intervjuene ser vi at flere av bedriftene har eller planlegger å innføre tiltak som bedrer IKT-sikkerheten deres. Vi konkluderer med at en bevissthetsøkning av nytteverdien vil bidra til å øke etterlevelsen av NSMs grunnprinsipper for IKT-sikkerhet.

Abstract

The purpose of *NSM's Cyber Security Principles in practice* is to help reduce the vulnerability of small and medium-sized enterprises (SMEs) to ICT security incidents.

ICT security work can be challenging for SMEs, which often have less resources and expertise than larger companies. The *Norwegian National Cyber Security Center* experiences that if businesses had implemented NSM's Cyber Security Principles to a greater extent, all incidents could have been avoided or the damage limited. To help reduce SMEs' vulnerability to ICT security incidents, we are therefore looking at how compliance with NSM's Cyber Security Principles can be increased.

Through in-depth interviews with 11 employees responsible for ICT security in each of their respective SMEs, we investigate what relationship they have with NSM's Cyber Security Principles and measure the extent to which the principles are adhered to. We also look at conditions that affect compliance and what challenges companies have with ICT security work. After the interviews, we follow up the informants with a survey.

The companies' routines and processes for backup comply with NSM's recommendations to a low to medium degree. This suggests that there is a need to increase compliance with NSM's basic principles and it may appear that the informants also saw a need for this. The awareness that was raised as a result of the interviews had great impact on the informants. Following the interviews, we see that several of the companies have or are planning to introduce measures that improve their ICT security. We conclude that an increase in awareness of the utility value will help to increase compliance with NSM's Cyber Security Principles.

Forord

Denne bacheloroppgaven *NSMs grunnprinsipper i praksis* er avslutningen på et spennende bachelorløp gjennom studieprogrammet digital infrastruktur og cybersikkerhet ved NTNU i Trondheim. Gjennom studieprogrammet har vi hatt flere emner innenfor informasjonsteknologi. Særlig givende fant vi de som omhandlet informasjonssikkerhet. Derfor var det naturlig for oss å skrive en bacheloroppgave innen dette fagfeltet.

Underveis i arbeidet med denne oppgaven har vi blitt kjent med mange mennesker med god kompetanse på informasjonssikkerhet. Vi har tilegnet oss verdifull kunnskap innen dette fagfeltet, og det har vært givende å kunne anvende denne kunnskapen.

Vi vil rette en stor takk til vår veileder Olav Skundberg, førstelektor ved NTNU i Trondheim for god veiledning i løpet av prosjektperioden.

I tillegg vil vi takke våre oppdragsgivere Roy Myhre og Christoffer Ottesen ved Sopra Steria i Trondheim for et godt samarbeid.

Til slutt vil vi takke alle som stilte opp til intervju. Deres åpenhet og tillitt til oss har vært viktig for oppgavens verdi. En spesiell takk til informanten som hjalp oss med å etablere kontakt med andre informanter fra sin bransje.

Innhold

Figurer

Tabeller

Akronymer

CIS	Center for Internet Security
CSC	Critical Security Controls
ICT	Information and communications technology
IEC	International Electrotechnical Commission
IKT	Informasjons- og kommunikasjonsteknologi
ISO	International Organization for Standardization
IT	Informasjonsteknologi
MFA	Multifaktorautentisering
NCSC	Nasjonalt cybersikkerhetssenter
NIST	National Institute of Standards and technology
NSM	Nasjonal sikkerhetsmyndighet
NSR	Næringslivet sikkerhetsråd
NTNU	Norges teknisk-naturvitenskapelige universitet
SMB	Små og mellomstore bedrifter
SME	Small and medium sized enterprises

Ordforklaringer

Dybdeintervju – Brukes som betegnelse på et kvalitativt intervju (også kalt semistrukturert intervju) som bærer preg av samtaler mellom intervjuer og informant [1, s. 287].

IKT-driftsleverandør – Eksternt firma som leverer IKT-tjenester. Når vi snakker om tjenesteutsetting av IKT-drift i denne oppgaven blir parten som har ansvar for IKT-driften omtalt som IKT-driftsleverandør.

IKT-sikkerhetshendelser - IKT hendelser, som fører til negative konsekvenser.

Informant – En person som man får informasjon eller opplysninger fra [2]. Alle personer vi har intervjuet i forbindelse med dette prosjektet vil omtales som informanter.

Informasjonssikkerhet – Omhandler å håndtere risiko relatert til bedriftens informasjonsverdier og behandling av personopplysninger [3].

Lagringsmedium - En elektronisk eller fysisk enhet for lagring av informasjon til bruk for senere lesing, lytting, framføring, overføring eller lignende [4].

Leverandørkjede - En leverandørkjede refererer til økosystemet av prosesser, mennesker, organisasjoner og distributører som er involvert i opprettelsen og leveringen av en endelig løsning eller produkt [5, s. 6].

Leverandørkjedeangrep – Et leverandørkjedeangrep er en kombinasjon av minst to angrep. Det første angrepet er på en leverandør som deretter brukes til å angripe målet for å få tilgang til eiendelene. Målet kan være sluttkunden eller en annen leverandør [5, s. 6].

Løsepengevirus – Også kalt *ransomware*, er en type skadelig programvare, som truer offeret sitt ved å ødelegge eller blokkere tilgangen til viktige data eller systemer inntil det betales løsepenger.

NSMs anbefalinger - Nasjonal sikkerhetsmyndighets grunnprinsipper for IKT-sikkerhet omtales ofte i denne oppgaven som NSMs anbefalinger.

NSMs grunnprinsipper - Nasjonal sikkerhetsmyndighets grunnprinsipper for IKT-sikkerhet.

Phishing – En form for sosial manipulering, der angriper forsøker å lure offeret til å utføre en handling. Dette kan være å åpne et vedlegg i en e-post eller klikke på en lenke. Vedleggene kan inneholde løsepengevirus [6].

Rammeverk for IKT-sikkerhet – En strukturert tilnærming til å beskytte informasjonsverdier og teknologiske systemer i en bedrift. Vi skiller ikke mellom rammeverk og styringssystem for IKT-sikkerhet i denne oppgaven.

Risiko - I informasjonssikkerhet snakker man om sannsynligheten for en hendelse og konsekvensen til hendelsen. Man tallfester sannsynligheten og konsekvensen ut ifra hvor alvorlige det er. Risikoen til en hendelse blir utregnet som sannsynligheten ganget med konsekvensen [7, s. 74-75].

Sikt – Er en tjenesteleverandør for kunnskapssektoren [8]. Det er Sikt som behandler søknad om behandling av personopplysninger.

Skadevare - Også kalt *malware, e*r et samlebegrep for skadelig programvare som kan brukes for å angripe IKT-systemer [7, s. 140].

Små og mellomstore bedrifter - I Norge er det vanlig å definere små og mellomstore bedrifter som bedrifter med under 100 ansatte.

Tjenesteutsetting – Når et foretak setter deler av sin produksjon til underleverandør [9]. Tjenesteutsetting blir også ofte omtalt som *outsourcing*.

1 Introduksjon

1.1 Bakgrunn

På bakgrunn av at Norge er et av verdens mest digitaliserte land, og at trusselaktører og angrepsformene deres blir mer sofistikerte, er det helt nødvendig at norske bedrifter tar IKT-sikkerhet på alvor.

I media hører man stadig vekk om dataangrep med alvorlige konsekvenser. Et eksempel på dette er Østre Toten kommune, da de i 2021 ble alvorlig rammet av et løsepengevirus. Dataangrepet førte blant annet til at personopplysninger om barn kom på avveie og personopplysningene ble tapt. Ordføreren mener at angrepet medførte et tap på 35 millioner kroner og i etterkant av hendelsen fikk kommunen 16 millioner i statsstøtte til oppryddingen [10]. Dette viste hvilke ringvirkninger hendelsen fikk for fellesskapet og hvor stor effekt gode rutiner og robust sikkerhetskopiering har, målt i kroner og øre. Kommunen hadde sikkerhetskopiering av viktige data, men de manglet beskyttelse av sikkerhetskopiene. Dermed ser vi at selv om sikkerhetskopi er essensielt for å forhindre datatap, er også gode rutiner og prosesser rundt sikkerhetskopiering like viktig.

Små og mellomstore bedrifter (SMB) blir stadig mer avhengig av informasjons- og kommunikasjonsteknologi (IKT) i sin daglige drift. I tillegg er SMB ofte underleverandører [11]. Underleverandører blir i økende grad utsatt for dataangrep og brukt som inngangsporter for cyberkriminelle til større bedrifter i såkalte leverandørkjedeangrep [12, s. 14-15]. Selv om SMB kanskje ikke har ressursene og ekspertisen til store organisasjoner når det gjelder IKT-sikkerhet, må de likevel ta dette på alvor for å beskytte sine informasjonsverdier og systemer. I denne sammenhengen er det derfor avgjørende at SMB forstår risikoen og tar hensiktsmessige tiltak for å beskytte seg mot disse truslene.

1.2 Formål

Formålet med oppgaven er å bidra til å redusere SMB sin sårbarhet til IKT-sikkerhetshendelser. Vi vil undersøke bedrifters modenhet når det kommer til IKT-sikkerhetsarbeid, og fokuset vil være praksiser som er knyttet til sikkerhetskopiering for å beskytte mot datatap.

1.3 Problem

Nasjonal Sikkerhetsmyndighet (NSM) har sett en tendens til at populære rammeverk for IKT-sikkerhet ikke alltid er optimale for SMB da de ofte er utviklet med tanke på større virksomheter [13]. Derfor har NSM utviklet NSMs grunnprinsipper for IKT-sikkerhet som inneholder et sett med prinsipper og tiltak for å «beskytte informasjonssystemer, data og tjenester mot uautorisert tilgang, skade, eller misbruk» [14].

Problemet er at små bedrifter ofte har mindre ressurser og kompetanse enn større bedrifter, derfor kan IKT-sikkerhetsarbeid være utfordrende. Et hjelpemiddel for å få en strukturert og metodisk tilnærming til IKT-sikkerhetsarbeid er å følge et rammeverk for

IKT-sikkerhet. Til tross for dette viser Mørketallsundersøkelsen at kun halvparten av SMB følger et rammeverk eller styringssystem for IKT-sikkerhet [15, s. 12-13].

1.3.1 Problemstilling

Nasjonalt cybersikkerhetssenter (NCSC) erfarer at «alle digitale hendelser kunne vært unngått eller skaden begrenset dersom virksomheter i større grad hadde implementert NSM Grunnprinsipper for IKT-sikkerhet» [16, s. 29]. SMB sin sårbarhet til IKT-sikkerhetshendelser vil derfor reduseres dersom de i større grad etterlever NSMs grunnprinsipper for IKT-sikkerhet. Vi har med det valgt følgende problemstilling:

*Hvordan kan man øke etterlevelsen av NSMs grunnprinsip*per for IKT-sikkerhet?

1.3.2 Forskningsspørsmål

For å besvare problemstillingen var vi nødt til å skaffe oss en oversikt over IKT-sikkerhetstilstanden hos SMB og avgjøre hvorvidt det er behov for å øke etterlevelsen. Vi vil ta utgangspunkt i sikkerhetskopieringspraksiser og bruke disse som en indikator på bedrifters modenhet og generelle IKT-sikkerhetstilstand. Derfor har vi valgt å undersøke hvorvidt bedrifters sikkerhetskopieringspraksiser samsvarer med NSM sine anbefalinger, og undersøke hvilke forhold som påvirker etterlevelsen. Vi har med det valgt følgende forskningsspørsmål:

Forskingsspørsmål 1

I hvilken grad samsvarer bedrifters rutiner og prosesser for sikkerhetskopiering med NSMs anbefalinger?

Forskningsspørsmål 2

Hvilke forhold påvirker etterlevelsen av NSMs anbefalinger?

1.4 Avgrensinger og rammer

SMB

Vi har valgt å avgrense oppgaven til bedrifter i SMB-markedet. Over 99 prosent av alle bedrifter i Norge regnes som SMB og de står for omtrent 70 prosent av verdiskapingen i privat sektor [17, s. 6]. Det er en generell antakelse om at IKT-sikkerhet er dårlig i SMB-markedet grunnet begrensede ressurser og kompetanse. Dette gjør det hensiktsmessig å studere dette området nærmere og bidra til forbedring.

Sikkerhetskopiering

Vi har valgt å avgrense hvordan vi vurderer bedrifters etterlevelse av NSMs grunnprinsipper for IKT-sikkerhet, til sikkerhetskopieringspraksiser. Bakgrunnen for dette er en antakelse fra vår side om at bedrifters modenhet på sikkerhetskopiering også gir en god pekepinn på bedrifters øvrige IKT-sikkerhetsarbeid. SMB-markedet består av bedrifter med forskjellig grad av modenhet når det kommer til IKT-sikkerhet. Siden sikkerhetskopi og prosessen rundt det er noe av det første man bør begynne med [18], og noe alle bedrifter uavhengig av modenhet må ta stilling til, vil det kunne gi oss sammenlignbare resultater.

NSMs Grunnprinsipper for IKT-sikkerhet

Vi ønsket å sammenligne bedrifters praksis med NSMs grunnprinsipper. Dette er et omfattende rammeverk som består av 21 grunnprinsipper med 118 tilknyttede tiltak.

For å gjøre intervjuene mer målrettet valgte vi å fokusere på spørsmål knyttet til etterlevelse av prinsipp 2.9 - *Etabler evne til gjenoppretting av data,* da dette er det mest relevante grunnprinsippet i forbindelse med sikkerhetskopiering.

Det var også hensiktsmessig å undersøke hvordan bedriftene forholder seg til tjenesteleverandører, da mange SMB helt eller delvis tjenesteutsetter sin IT-drift. Dermed vil deler av oppgaven også fokusere på prinsipp 2.1 - *Ivareta sikkerhet i anskaffelses- og utviklingsprosesser.*

Forskningsmetode og Informanter

Utvalget av informanter ble avgrenset til ansatte i SMB med en grad av ansvar for IKT-sikkerhet. Metoden som ble brukt for å undersøke bedrifters praksis rundt sikkerhetskopiering ble avgrenset til dybdeintervjuer. Vi benyttet et spørreskjema for å undersøke effekten av intervjuene.

1.5 Målgruppe

Målgruppen til oppgaven er norske digitaliserte bedrifter, herunder IT-personell og ansatte i ledelsen. Oppgaven fokuserer særlig på bedrifter innenfor SMB segmentet, men eventuelle funn kan i tillegg være av interesse for større virksomheter. Videre kan funn gjennom intervjuprosessen være av interesse for NSM.

1.6 Rapportstruktur

1. **Introduksjon -** Her forklares bakgrunnen for prosjektet, formålet med oppgaven, hvilket problem vi ønsker å løse og rammene for oppgaven blir presentert.
2. **Teori -** Her presenteres sentral teori som ligger til grunn for vår besvarelse av oppgaven. Teorien i kapittelet blir presentert på en måte som gir leseren mulighet til å skjønne hva som ligger bak besvarelsen, slik at oppgaven kan forstås av personer uten IT-kompetanse.
3. **Metode –** Her beskrives hvordan vi har gått fram for å besvare oppgaven. Vi vil presentere de forskjellige metodene og tilnærmingene vi har brukt for å samle inn, analysere og tolke data.
4. **Resultater –** Her presenteres resultatene vi har fått fra intervjuene.
5. **Diskusjon –** Her diskuterer vi resultatene fra intervjuene og benytter disse til å besvare forskningsspørsmålene.
6. **Konklusjon –** Her oppsummeres funnene vi har gjort og konkluderer problemstillingen. Til slutt ser vi på videre arbeid.

2 Teori

2.1 Introduksjon

I teorikapittelet vil vi først presentere teori om rammeverk og styringssystem for IKT-sikkerhet, her vil fokuset være NSMs grunnprinsipper for IKT-sikkerhet. Videre vil vi presentere teori om sikkerhetskopiering og tjenesteutsetting. Avslutningsvis trekker vi frem funn fra Mørketallsundersøkelsen relatert til IKT-sikkerhetstilstanden hos SMB.

2.2 Rammeverk og styringssystem for IKT-sikkerhet

Når vi snakker om rammeverk og styringssystem for IKT-sikkerhet deler NSM disse inn i to kategorier, styringsrammeverk og tiltaksrammeverk [19, s. 8]. Et styringsrammeverk omhandler den strategiske og organisatoriske siden av informasjonssikkerhet, mens et tiltaksrammeverk fokuserer på de praktiske og tekniske sidene ved informasjonssikkerhet. Overordnet kan vi si at et rammeverk for IKT-sikkerhet er en strukturert tilnærming til å beskytte informasjonsressurser og teknologiske systemer i en bedrift. Et slikt rammeverk bør inneholde retningslinjer, beste praksis, prinsipper, prosedyrer og kontroller som hjelper bedrifter med IKT-sikkerhet. Vår oppgave dreier seg i stor grad om NSMs grunnprinsipper for IKT-sikkerhet. Derfor vil vi detaljert beskrive hensiktsmessige deler av dette rammeverket, i tillegg til en kort beskrivelse av noen andre anbefalte og anerkjente rammeverk for IKT-sikkerhet.

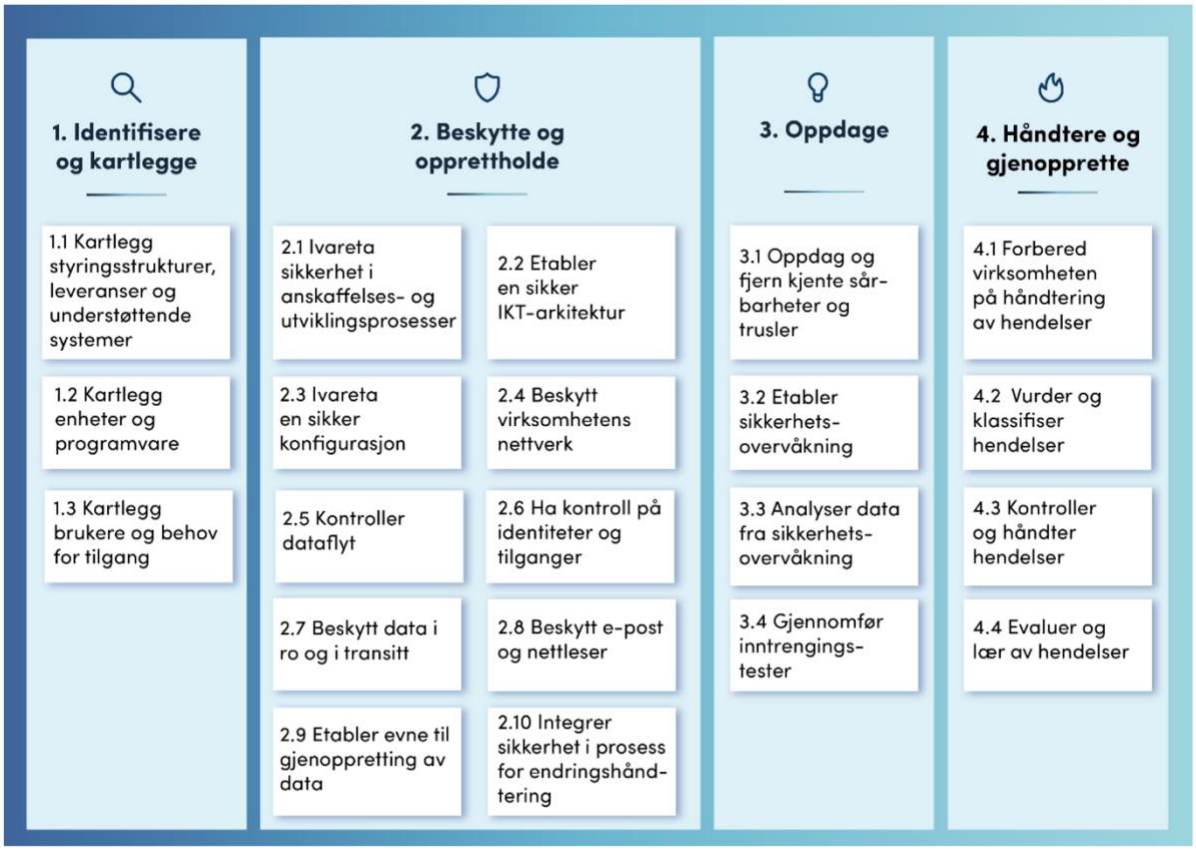
2.2.1 NSMs grunnprinsipper for IKT-sikkerhet

NSM har i samarbeid med norske private og offentlige virksomheter utarbeidet et sett med prinsipper og tiltak for å beskytte informasjonssystemer mot uautorisert tilgang, skade eller misbruk. Nyeste versjon er *NSMs Grunnprinsipper for IKT-sikkerhet versjon 2.0* som ble utgitt 15. april 2020 [19].

Selv om hovedmålgruppen er virksomheter som forvalter kritiske samfunnsfunksjoner og/eller kritisk infrastruktur, presiserer NSM at grunnprinsippene er relevante for alle offentlige og private virksomheter, uavhengig av om de forvalter informasjonssystemene selv eller ved hjelp av en tredjepart og uavhengig av om virksomheten er underlagt sikkerhetsloven [19, s. 4].

Grunnprinsippene består av teknologiske og organisatoriske tiltak som NSM mener er mest relevante for at norske virksomheter skal kunne etablere et godt forsvar mot cybertrusler. Totalt er det 118 sikkerhetstiltak, fordelt på 21 prinsipper. Selv om grunnprinsippene skal beskytte mot handlinger uavhengig av motivasjon, så er hovedfokuset på tilsiktede handlinger [19, s. 5].

De 21 prinsippene fra NSMs grunnprinsipper for IKT-sikkerhet er fordelt på fire kategorier. For hver kategori beskriver NSM den overordnede målsetningen. *Figur* 2.1*,* hentet fra NSMs grunnprinsipper for IKT-sikkerhet, viser kategoriene med tilhørende prinsipper [19, s. 6].



Figur 2.1: NSMs Grunnprinsipper for IKT-sikkerhet

For hvert grunnprinsipp beskriver NSM:

- Hva virksomheter oppnår ved å innføre prinsippet.
- Viktigheten av prinsippet og mulige konsekvenser dersom det ikke blir etterfulgt.
- Konkrete sikkerhetstiltak virksomheter bør iverksette for å etterleve prinsippet.
- Annen relevant informasjon og kilder relatert til prinsippet.

Støtteprodukter til NSMs Grunnprinsipper for IKT-sikkerhet

NSM har utarbeidet et regneark som støtteprodukt, for å bistå virksomheter i arbeidet med å implementere grunnprinsippene for IKT-sikkerhet. Regnearket samler alle sikkerhetstiltakene for hvert grunnprinsipp og inneholder i tillegg prioritering av sikkerhetstiltakene og hvordan de er koblet til ISO/IEC 27002. Hvert tiltak i regnearket er prioritert fra 1 til 3 basert på hva som etter NSMs erfaring gir sikkerhetsmessig størst effekt [20].

Prioriteringsgruppe 1 består av de høyest prioriterte sikkerhetstiltakene, som en virksomhet bør implementere så snart som mulig. Disse tiltakene er svært viktige for å beskytte organisasjonens sensitive data og systemer. Manglende implementering av noen av disse tiltakene kan være roten til vellykkede dataangrep, og kan føre til betydelig skade på virksomheten. Tiltakene i denne gruppen er vanligvis enkle å implementere og krever ikke store investeringer eller organisatoriske endringer. Derimot kan noen av tiltakene kreve kultur- og holdningsendringer blant de ansatte, for å sikre at de tar sikkerheten på alvor [20].

Prioriteringsgruppe 2 består av mer viderekommende sikkerhetstiltak som en virksomhet kan implementere. Disse tiltakene kan være mer komplekse å implementere og kreve mer tid og ressurser enn tiltakene i Prioriteringsgruppe 1. Det er viktig å merke seg at en virksomhet bør ha en plan for implementering av tiltakene i Prioriteringsgruppe 1 før man begynner å bruke store ressurser på tiltakene i Prioriteringsgruppe 2 [20].

Prioriteringsgruppe 3 består av øvrige sikkerhetstiltak som en virksomhet kan implementere for å forbedre sin totale sikkerhet. Det er viktig å merke seg at en virksomhet bør ha en plan for implementering av tiltakene i både Prioriteringsgruppe 1 og 2 før man begynner å bruke store ressurser på tiltakene i Prioriteringsgruppe 3 [20].

Prinsipp 2.9 Etabler evne til gjenoppretting av data

Prinsipp 2.9 har som mål at «virksomheter skal etablere en metode for sikkerhetskopiering og gjenoppretting av kritiske data for å hindre tap» [19, s. 34].

NSM begrunner viktigheten av prinsippet med:

> Virksomheten bør etablere kapasitet for å gjenopprette tapte eller endrede data og systemkonfigurasjoner. Enkelte dataangrep medfører at kritiske konfigurasjoner, programvare eller informasjon endres eller gjøres utilgjengelig. Dette kan påvirke virksomhetskritiske prosesser. Et eksempel på et slikt angrep er kryptovirus, der både informasjon og det underliggende systemet kan bli kryptert og dermed blir utilgjengelig. [19, s. 34]

For prinsipp 2.9 anbefaler NSM følgende tiltak [19, s. 35]:

ID	Beskrivelse	Prioritet
2.9.1	**Legg en plan for regelmessig sikkerhetskopiering av alle virksomhetsdata.** En slik plan bør som minimum beskrive: **a)** Hvilke data som skal sikkerhetskopieres. **b)** Regelmessighet på sikkerhetskopiering av ulike data, basert på verdi. **c)** Ansvar for sikkerhetskopiering av ulike data. **d)** Prosedyrer ved feilet sikkerhetskopiering. **e)** Oppbevaringsperiode for sikkerhetskopier. **f)** Logiske og fysiske krav til sikring av sikkerhetskopier. **g)** Krav til gjenopprettingstid for virksomhetens ulike systemer og data (se prinsipp 4.1 - Forbered virksomheten på håndtering av hendelser). **h)** Godkjenningsansvarlig(e) for planen.	1
2.9.2	**Inkluder sikkerhetskopier av programvare** for å sikre gjenoppretting. Dette inkluderer (som minimum) **a)** sikkerhetskonfigurasjon ref. prinsipp 2.3 - Ivareta en sikker konfigurasjon og **b)** maler for virtuelle maskiner og «master-images» av operativsystemer og **c)** Innstallasjonsprogramvare.	3
2.9.3	**Test sikkerhetskopier regelmessig** ved å utføre gjenopprettingstest for å verifisere at sikkerhetskopien fungerer.	2
2.9.4	**Beskytt sikkerhetskopier mot tilsiktet og utilsiktet sletting, manipulering og avlesning.** **a)** Sikkerhetskopier bør være separert fra virksomhetens produksjonsmiljø. Se bl.a. prinsipp 2.1 - Ivareta sikkerhet i anskaffelses- og utviklingsprosesser. **b)** Tilgangsrettigheter til sikkerhetskopier bør begrenses til kun ansatte og	3

	systemprosesser som skal gjenopprette data. **c)** Det bør jevnlig tas offline sikkerhetskopier som ikke kan nås via virksomhetens nettverk. Dette for å hindre tilsiktet/utilsiktet sletting eller manipulering. **d)** Sikkerhetskopier bør beskyttes med kryptering når de lagres eller flyttes over nettverket. Dette inkluderer ekstern sikkerhetskopiering og skytjenester.	

Tabell 2.1: Tiltak fra prinsipp 2.9 Etabler evne til gjenoppretting av data, sammenstilt med prioriteringsgruppen tiltakene tilhører.

Prinsipp 2.1 Ivareta sikkerhet i anskaffelses- og utviklingsprosesser

Prinsipp 2.1 har som mål at «Sikkerhet er en integrert del av prosessene for anskaffelse og utvikling og virksomheten minimerer risiko for at nye IKT-produkter og IKT-tjenester innfører konfigurasjonsmessige og arkitekturmessige sårbarheter» [19, s. 18].

NSM begrunner viktigheten av prinsippet med:

> IKT-sikkerhet er viktig i alle IKT-produkter og IKT-tjenester, ikke kun ved anskaffelse av rene sikkerhetsprodukter som en brannmur. Dersom en virksomhet anskaffer IKT-produkter og IKT-tjenester som har svak sikkerhet eller som ikke integrerer godt med virksomhetens øvrige sikkerhetsarkitektur og eksisterende IKT-produkter, kan dette øke sårbarheten og redusere sikkerhetsnivået i IKT-systemet. [19, s. 18]

For prinsipp 2.1 anbefaler NSM 10 tiltak, vi har valgt følgende av disse [19, s. 18-20]:

ID	Beskrivelse	Prioritet
2.1.9	**Ta ansvar for virksomhetens sikkerhet også ved tjenesteutsetting.** Dette inkluderer å **a)** ha oversikt og kontroll på hele livsløpet til tjenesten(e) som skal settes ut, **b)** ivareta behovet for bestillerkompetanse (f.eks. forvaltning-, administrasjon- og IT-arkitekturkompetanse) gjennom hele livsløpet til tjenesteutsettingen **c)** gjennomføre gode risikovurderinger som inkluderer IKT og hensyntar hele livsløpet, **d)** utarbeide et kravdokument for alle faser av tjenesteutsettingen hvor krav kan verifiseres, **e)** avtaler om tjenesteutsetting av IKT-tjenester og endringer i slike avtaler skal behandles i henhold til virksomhetens fullmaktsstruktur. Det understrekes at virksomhetens ansvar for sikkerheten ikke forsvinner selv om man tjenesteutsetter. Virksomheten har et ansvar uavhengig av hvem som utfører de forskjellige oppgavene.	1
2.1.10	**Undersøk sikkerheten hos tjenesteleverandør ved tjenesteutsetting**. Det bør som minimum undersøkes om leverandøren: **a)** har et etablert styringssystem for informasjonssikkerhet og eventuelt sertifisering i henhold til internasjonale standarder, for eksempel ISO/IEC 27001:2017. **b)** gir innsyn i sikkerhetsarkitekturen som benyttes for å levere tjenesten.	3

	c) har utviklingsplaner for fremtidig sikkerhetsfunksjonalitet i tjenestene i tråd med utvikling i teknologi og trusselbildet over tid. **d)** har en oversikt over hvem som skal ha innsyn i virksomhetens informasjon, hvor og hvordan denne skal behandles og lagres samt grad av mekanismer for segregering fra andre kunder. **e)** har sikkerhetsfunksjonalitet som tilfredsstiller virksomhetens behov. **f)** har sikkerhetsovervåkning for å avdekke sikkerhetshendelser som kan påvirke virksomheten. **g)** har rutiner for hendelseshåndtering og avviks- og sikkerhetsrapportering. **h)** har krise- og beredskapsplaner som skal harmonisere med virksomhetens egne planer. **i)** har godkjenningsprosedyrer for bruk av underleverandører og deres bruk av underleverandører. **j)** har spesifisert hvilke aktiviteter som skal utføres ved terminering av kontrakten, blant annet tilbakeføring/flytting/sletting av virksomhetens informasjon.	

Tabell 2.2: Tiltak fra prinsipp 2.1 Ivareta sikkerhet i anskaffelses- og utviklingsprosesser. Sammenstilt med prioriteringsgruppen tiltakene tilhører.

2.2.2 Andre etablerte rammeverk for IKT-sikkerhet

ISO/IEC 27001:2017

ISO/IEC 27001 er en internasjonal standard for implementering av styringsrammeverk for IKT-sikkerhet, utarbeidet av Den internasjonale standardiseringsorganisasjon (ISO) og Den internasjonale elektroniske kommisjon (IEC) [21, s. 2].

ISO/IEC 27002:2013

ISO/IEC 27002 er en internasjonal standard utarbeidet av ISO og IEC som beskriver sikringstiltak for informasjonssikkerhet [22, s. 5-7]. NSM kategoriserer ISO/IEC 27002 som et tiltaksrammeverk og tiltakene i NSMs grunnprinsipper er tett knyttet opp mot denne standarden [19, s. 7].

NIST Cybersecurity framework

NIST Cybersecurity framework er et tiltaksrammeverk utviklet av National Institute for Standards and Technology (NIST) og er bygd på eksisterende standarder, retningslinjer og praksiser. Rammeverket er delt opp i fem hovedfunksjoner – identifisere, beskytte, oppdage, respondere og gjenopprette. Disse hovedfunksjonene vil til sammen gi et omfattende overblikk over livssyklusen for håndtering av IT-trusler over tid [23].

CIS Critical Security Controls

CIS Critical Security Controls er et initiativ ledet av Center for Internet Security (CIS) for å identifisere de mest vanlige og viktigste cyberangrepene mot virksomheter. Resultatet av dette initiativet er CIS Critical Security Controls, som er et tiltaksrammeverk hvor

målet er å hjelpe bedrifter med å prioritere de viktigste tiltakene, for å beskytte seg mot de mest skadelige angrepene [24, s. 1].

2.3 Sikkerhetskopiering

Innen informasjonssikkerhet finnes det tre grunnpilarer, ofte referert til som CIA [25]:

- *Konfidensialitet*, som omhandler at informasjonen ikke blir kjent for uvedkommende [26, s. 21].
- *Integritet*, som omhandler at informasjonen ikke blir endret utilsiktet, eller av uvedkommende [26, s. 22].
- *Tilgjengelighet*, som omhandler at informasjonen er tilgjengelig for autoriserte personer ved behov [26, s. 23].

Sikkerhetskopi er kopier av data, som brukes til å gjenopprette dataene i tilfelle data går tapt, dataen blir korrupt eller dataen blir utilgjengelig [27, s. 237]. En god sikkerhetskopieringspraksis vil være med å styrke en bedrifts evne til å opprettholde tilgjengeligheten og integriteten til virksomhetskritisk og sensitiv data.

2.3.1 Hvorfor ta sikkerhetskopi?

Det en virksomhet i bunn og grunn ønsker å sikkerhetskopiere kalles informasjonsverdier. En informasjonsverdi er mengde informasjon som blir definert og behandlet sammen som en enhet, slik at den kan bli forstått, delt og beskyttet effektivt [28, s. 10].

For å vurdere om en mengde data er en informasjonsverdi, kan virksomheten stille seg selv følgende spørsmål [28, s. 11]:

- Har dataen verdi for virksomheten?
- Vil det være legale, omdømmemessige eller finansielle konsekvenser dersom virksomheten mister tilgang til dataen?
- Vil det påvirke den operasjonelle driften dersom virksomheten mister tilgang?

Når vi nå vet hva som kjennetegner en informasjonsverdi, er det tydelig hvorfor det er behov for sikkerhetskopi av disse, da mulige konsekvenser av tapte eller utilgjengelige informasjonsverdier kan ha ringvirkninger som [29, s. 8-10]:

- **Tap av kunder** – Enten om kundedatabasen går tapt, eller om datatap fører til at kunder mister tillitt til virksomheten og går til en konkurrent.
- **Tapt tid** – Enten om det tar lang tid å gjenopprette tapt data, eller om data er permanent tapt og arbeidet må gjøres på nytt, fører det til tapt tid som kunne blitt brukt på annen verdiskapning.
- **Tap av moral** – Moral hos ansatte kan svekkes dersom deres arbeid går tapt, dette kan igjen føre til lavere produktivitet.
- **Svekket rykte** – Bedrifter som utsettes for datatap kan få et dårlig rykte, som kan føre til at kunder heller går til konkurrenter.

Det er en rekke uønskede hendelser som kan medføre brudd på konfidensialiteten, integriteten eller tilgjengeligheten til informasjonsverdier. Ved å inneha gode sikkerhetskopieringspraksiser kan en redusere konsekvensen av dette. Eksempler på slike uønskede hendelser er:

- **Feil ved lagringsmedium** – både logiske og fysiske feil kan forekomme ved lagringsmedium og medføre at dataen blir korrupt.
- **Tyveri/Tilsiktet sletting** – Fysiske lagringsmedium kan bli stjålet, eller data kan bli stjålet digitalt og deretter slettet.
- **Utilsiktet sletting** - Alt som kreves er at en person er uheldig, så kan viktige filer være slettet for godt.
- **Insidere** – Misfornøyde ansatte kan hevne seg ved å slette data.
- **Naturkatastrofer** – Kan føre til ødeleggelse av lagringsmedium.
- **Skadevare** – Eksempelvis løsepengevirus som krypterer data.

I tillegg kan sikkerhetskopier brukes for arkiveringsformål. Det vil si at man har en total sikkerhetskopi av sentrale data for hvert år, slik at man ved behov har tilgang.

Løsepengevirus

Løsepengevirus er en type skadevare, som gjør informasjonsverdier utilgjengelig for offeret. Angriperen krever ofte en betydelig pengesum for å tilgjengeliggjøre det som er kryptert, men offeret har ingen garanti for at det skjer, selv om vedkommende betaler.

Løsepengevirus deles inn i to hovedgrupper, krypteringsvirus og låsevirus [30]:

1. **Krypteringsvirus** krypterer sensitive filer og data og hindrer på denne måten offeret tilgang, i tillegg er det noen versjoner som også truer med å lekke sensitive opplysninger med mindre offeret betaler.
2. **Låsevirus** låser brukeren ut fra enheten og krever betaling for å låse opp.

Det er mange måter å beskytte seg mot å bli infisert av et løsepengevirus, men et viktig aspekt er at en god sikkerhetskopieringsstrategi er det eneste tiltaket som kan forsikre om at data ikke går tapt, om man blir infisert.

En strategi som mange løsepengevirus i dag bruker, er å først lokalisere og kryptere sikkerhetskopiene, deretter resten av filene. På denne måten vil offeret få et større insentiv til å betale, da vedkommende ikke har mulighet til å gjenopprette fra sikkerhetskopi. Derfor holder det ikke bare med å ha sikkerhetskopi, man må også beskytte sikkerhetskopiene, helst separert fra nettverket om man skal være trygg [30].

2.3.2 Hvordan skal man sikkerhetskopiere?

Etter man har identifisert informasjonsverdiene man ønsker å ta sikkerhetskopi av, er man nødt til å avgjøre hvordan dette skal gjennomføres. Her bør det første man gjør, være å bestemme seg for om man ønsker å tjenesteutsette arbeidet med sikkerhetskopiering, eller om man ønsker å jobbe med sikkerhetskopiering internt i bedriften.

Dersom man velger å drifte sikkerhetskopiering innad i bedriften, er en god strategi man kan følge 3-2-1 prinsippet. Dette prinsippet er en strategi for sikkerhetskopiering, hvor poenget er å redusere den potensielle effekten av datatap. Strategien går ut på at du alltid skal ha 3 kopier av data, 2 av kopiene skal være lagret lokalt, men på forskjellige lagringsmedium, og 1 kopi skal være lagret på en lokasjon et annet sted enn de andre [31].

Dersom man velger å drifte sikkerhetskopiering innad i bedriften, er en god strategi man kan følge 3-2-1 prinsippet. Dette prinsippet er en strategi for sikkerhetskopiering, hvor

poenget er å redusere den potensielle effekten av datatap. Strategien går ut på at du alltid skal ha 3 kopier av data, 2 av kopiene skal være lagret lokalt, men på forskjellige lagringsmedium, og 1 kopi skal være lagret på en lokasjon et annet sted enn de andre [31]. Selv om 3-2-1 prinsippet er en god introduksjon til sikkerhetskopiering, bør denne bare bli sett på som et absolutt minimum for hvordan man skal sikkerhetskopiere. Dessuten beskriver ikke denne strategien spesifikt hvordan man skal beskytte sikkerhetskopiene.

For å sikre konfidensialitet, integritet og tilgjengelighet, er beskyttelse av sikkerhetskopiene viktig. NSMs tiltak 2.9.4 inneholder fire viktige punkter som er sentrale for beskyttelse av sikkerhetskopier [19, s. 35]:

a) *Separer sikkerhetskopiene fra produksjonsmiljø*

Menneskestyrte løsepengevirus begynner ofte med at trusselaktører stjeler kontolegitimasjon, og dermed opparbeider seg tilgang til bedriftens produksjonsmiljø [30]. Vi nevnte tidligere at noe av det første trusselaktører forsøker å gjøre ved et løsepengevirus, er å lokalisere og kryptere sikkerhetskopiene. Dersom sikkerhetskopiene ikke er tilgjengelig fra produksjonsmiljø, vil det bli vanskeligere for aktørene å få tilgang til dem. Det er derfor hensiktsmessig å separere sikkerhetskopiene fra produksjonsmiljøet.

Dette kan man for eksempel gjøre ved å ha en egen dedikert server, som er på et nettverk som er separert fra nettverket som brukes i produksjonsmiljøet. Dessuten kan disse plasseres på et annet sted enn der bedriften jobber. Dermed er man også bedre rustet i tilfelle det blir brann eller annen skade på arbeidslokale.

Bruk av skytjenester for sikkerhetskopiering er også en god tilnærming til dette. Om man har sikkerhetskopiene sine i skyen, vil de være separert fra produksjonsmiljøet, både når det kommer til at det er på et annet nettverk, men også ved at skyleverandøren har serverne sine på en annen geografisk lokasjon enn der arbeidslokalet til bedriften ligger.

b) *Begrens tilgangsrettigheter til personer og systemprosesser som skal gjenopprette data*

For å gjøre angrepsflaten til menneskestyrte løsepengevirus mindre, så bør man begrense tilgangen til sikkerhetskopiene og systemprosessene relatert til sikkerhetskopiene. Det er kun ansatte med ansvar for sikkerhetskopiering og gjenoppretting, som bør inneha tilgangsrettigheter til sikkerhetskopiene. Da vil trusselaktører kun få tilgang til sikkerhetskopiene, dersom de får tilgang på kontolegitimasjonen til en administrator. Dette vil også være med på å redusere sjansen for tilsiktet og utilsiktet sletting eller endring av sikkerhetskopier.

c) *Det bør jevnlig tas offline sikkerhetskopier*

Selv bedrifter som etterlever punkt a) og b) kan være sårbare for at trusselaktører krypterer sikkerhetskopiene. Dersom bedrifter oppbevarer sikkerhetskopier offline vil det være krevende for trusselaktører å kryptere dem, det vil kreve fysisk tilgang til sikkerhetskopiene. Dette er bakgrunnen for at NSM anbefaler at man jevnlig tar offline sikkerhetskopier. En offline sikkerhetskopi kan oppnås ved at en tar sikkerhetskopi av informasjonsverdier på lagringsmedium som ikke er tilkoblet nettverket.

d) *Sikkerhetskopier bør beskyttes med kryptering når de lagres eller flyttes over nettverket.*

Det vil være mer krevende for trusselaktører å lese dataen fra sikkerhetskopiene, dersom de er kryptert. På den måten, øker man sannsynligheten for at konfidensialiteten til informasjonsverdien bevares. Vi nevnte tidligere at noen trusselaktører i forbindelse med løsepengevirus, truer med å lekke sensitive opplysninger. Denne konsekvensen reduseres ved å kryptere sikkerhetskopiene.

Ved å kryptere sikkerhetskopier når man lagrer dem eller flytter dem over nettet, sørger man for at selv om noen får tak i sikkerhetskopiene, så vil avlesning av dataen være mye mer utfordrende.

2.4 Tjenesteutsetting av IT-drift

Hva som inngår i virksomheters IT-drift, vil variere basert på behov og digitale systemer i bruk. IT-drift kan eksempelvis omfatte drift av servere, nettverk og nettverksadministrasjon, sikkerhetskopiering og brukerstøtte. Det er sentralt at IKT-sikkerhet tas hensyn til og ivaretas kontinuerlig, når man jobber med IT-drift.

I en digitalisert virksomhet kan IT-drift være organisert internt, helt tjenesteutsatt, eller delvis tjenesteutsatt [15, s. 11]. Tjenesteutsetting av IT-drift innebærer å sette administrasjon og vedlikehold av IT-systemer til en ekstern leverandør. Dette er en strategi som mange virksomheter velger for å redusere kostnader, få tilgang til kompetanse de mangler i virksomheten og for å kunne konsentrere seg om sin kjernevirksomhet [32, s. 47].

NSMs grunnprinsipper inneholder veiledning når det kommer til tjenesteutsetting. Under prinsipp *2.1 Ivareta sikkerhet i anskaffelses- og utviklingsprosesser* beskrives konkrete anbefalinger og tiltak for tjenesteutsetting. Spesielt relevant er tiltak 2.1.9 *Ta ansvar for virksomhetens sikkerhet også ved tjenesteutsetting.* Dette tiltaket er i prioriteringsgruppe 1. I dette tiltaket understrekes det at ansvaret for IKT-sikkerheten bevares ikke forsvinner, selv om en tjenesteutsetter [19, s. 20].

For å sikre at virksomhetens behov ivaretas ved tjenesteutsetting av IT-drift, vil god bestillerkompetanse være en forutsetning. I tillegg er det fordelaktig å jevnlig kontrollere leverandøren, for å sørge for at arbeidet blir utført i henhold til avtalen. Under vil vi beskrive bestillerkompetanse og leverandørkontroll ytterligere.

2.4.1 Bestillerkompetanse

God bestillerkompetanse er en forutsetning for vellykket tjenesteutsetting av IT-drift. Utilstrekkelig bestillerkompetanse kan føre til anskaffelse av IKT-tjenester uten at behovet i tilstrekkelig grad er kartlagt og det kan derfor bli utfordrende å sette krav til leverandøren, blant annet når det kommer til IKT-sikkerhet [33].

God bestillerkompetanse innebærer en rekke ferdigheter og kunnskaper som er viktige for å sikre at virksomheten får mest mulig ut av sin tjenesteutsetting-strategi. I tillegg til grunnleggende IKT-kompetanse, anbefaler NSM fem kompetanseområder. Disse kompetanseområdene blir vist i *Figur* 2.2 [33].

VIRKSOMHETSKOMPETANSE	SIKKERHETSKOMPETANSE	INTEGRASJONSKOMPETANSE	KOMPETANSE OM ANSKAFFELSER	JURIDISK KOMPETANSE
- For å kunne definere behov og stille nødvendige krav.	- For å kunne vurdere risiko og stille riktige sikkerhetskrav. Dette gjelder alle områder av sikkerhet dvs. fysisk, personell- og informasjons-sikkerhet.	- For å kunne forstå hvordan tjenestene kan integreres i virksomheten på best mulig måte.	- Slik at anskaffelsen kan gjennomføres på en måte som støtter virksomhetens forretnings-messige og funksjonelle behov på best måte.	- Slik at virksomhetens juridiske krav og behov ivaretas og at kontrakten kan oppfylles i produksjonen.

Figur 2.2: Kompetanseområder som NSM anbefaler for å sikre god bestillerkompetanse

2.4.2 Leverandørkontroll

Leverandørkontroll går ut på å kontrollere en ekstern tjenesteleverandør, for å forsikre at avtaler opprettholdes og at tjenestene blir levert med god kvalitet. Å utføre leverandørkontroll er viktig for de bedriftene som helt eller delvis tjenesteutsetter sin IT-drift.

Leverandørkontroll omfatter blant annet overvåkning av leverandørens tjenester, for å forsikre seg om at de opprettholder avtalt kvalitet, i tillegg til kontinuerlig kontroll og evaluering av leverandørens ytelse [32, s. 142-144].

I prosessen med leverandørkontroll og ivaretakelse av god IKT-sikkerhet i forbindelse med tjenesteutsetting, kan virksomheter se til NSMs anbefalinger fra tiltak 2.1.9 og 2.1.10 [19, s. 19-20].

2.5 Mørketallsundersøkelsen

Næringslivet Sikkerhetsråd (NSR) utgir annethvert år Mørketallsundersøkelsen, hvor sikkerhetshendelser og sikkerhetsarbeid hos norske virksomheter kartlegges. Undersøkelsen har til hensikt å tilgjengeliggjøre statistikk på et område som virksomheter selv er forsiktige med å offentliggjøre. Undersøkelsen gjennomføres i form av en spørreundersøkelse, der respondentene representerer virksomheter med 5 ansatte eller mer, fra de fleste bransjer. I 2022-utgaven av Mørketallsundersøkelsen svarte totalt 2500 respondenter, hvorav 2234 av disse jobber for private virksomheter og 266 for offentlige virksomheter [15].

I mørketallsundersøkelsen kommer det frem at halvparten av virksomhetene har et rammeverk eller styringssystem for informasjonssikkerhet, 37 prosent svarer nei og 12 prosent vet ikke. Andelen som følger et rammeverk for IKT-sikkerhet, er høyere blant de store virksomhetene enn de små. Virksomhetene som følger et rammeverk eller styringssystem for IKT-sikkerhet, oppdager i større grad sikkerhetsbrudd ved rutinemessig intern sikkerhetsovervåkning, enn de som ikke har det, andelen ligger henholdsvis på 47 prosent og 28 prosent. De som ikke følger et rammeverk oppdager derimot slike hendelser i større grad ved en tilfeldighet eller via medieoppslag [15, s. 22].

Det kommer også frem at 43 prosent av virksomhetene har organisert IT-driften internt, 33 prosent har delvis tjenesteutsatt IT-drift og 22 prosent har helt tjenesteutsatt IT-drift. Den siste 3 prosenten vet ikke hvordan IT-driften organiseres.

Andre relevante funn for oppgaven er:

- 63 av 2500 respondenter oppgir at de har opplevd løsepengevirus i 2021 [15, s. 17].
- 1 prosent opplevde hendelser forårsaket av IKT-driftsleverandør [15, s. 15].

3 Metode

3.1 Introduksjon

For å besvare problemstillingen og tilhørende forskningsspørsmål, gjennomførte vi 11 dybdeintervjuer, og fulgte opp med en oppfølgingsundersøkelse. Metodene vi har benyttet i den anledning beskrives i dette kapittelet.

3.2 Metode for datagenerering

Innen samfunnsforskning fremstår kvalitativ og kvantitativ forskning som to vesentlige tenkemåter [1, s. 26]. Det er tidligere blitt studert og publisert data på IKT-sikkerhets tilstanden hos norske bedrifter og majoriteten av denne dataen er innhentet gjennom kvantitative forskningsmetoder. Kvantitativ forskning innehar fordelen med at det er mulig å innhente og systematisere informasjon fra store informantgrupper [34]. Det er derimot krevende å besvare forskningsspørsmålene våre ut fra kvantitativ data. For å gjøre en vurdering av hvorvidt bedrifters rutiner og prosesser samsvarer med NSM anbefalinger og for å indentifisere forhold som påvirker etterlevelsen, trengte vi tilstrekkelig og formålstjenlig data. Vi anså kvalitativ forskningsmetode og dybdeintervju som mest hensiktsmessig for dette.

Dybdeintervju er godt egnet for å generere informasjon om intervjukandidatene sine subjektive meninger, holdninger og erfaringer [1, s. 128]. Dersom intervjuer stiller åpne spørsmål vil intervjusituasjonen tillate digresjoner og muliggjøre for at informanten kan komme inn på temaer som forskningsgruppen ikke har tenkt på i forkant av intervjuet [1, s. 128]. Vi anså disse forholdene ved dybdeintervju som fordelaktige for å besvare vår oppgave. Metodevalget muliggjorde at vi kunne opparbeide oss en inngående forståelse av hvordan informantene praktiserte sikkerhetskopiering og hvilke utfordringer de støtte på i den anledning. Dybdeintervju la med det til rette for at vi kunne si noe om:

- Hvordan tilstanden er i dag
- Hvorfor den er slik
- Hvordan den kan forbedres

Videre legger metodevalget til rette for muligheten til følgende:

- Stille oppfølgingsspørsmål basert på intervjuobjektets svar.
- Forsikre om intervjuobjektenes kvalifikasjoner til å besvare spørsmålene.
- Presisere uklarheter for å påse at intervjuobjektene tolker spørsmålene likt, slik at datagrunnlaget for oppgaven blir pålitelig.

3.3 Utarbeiding av intervjuguide

Som et hjelpemiddel for gjennomføringen av intervjuene, utarbeidet vi en intervjuguide med et utvalg forhåndsdefinerte spørsmål. Det var essensielt for oss å utarbeide en intervjuguide som ville gi oss de nødvendige dataene for å kunne besvare vår problemstilling. For å oppnå dette studerte vi teori om sikkerhetskopiering og NSMs grunnprinsipper for IKT-sikkerhet.

Teoristudiene i seg selv var ikke dekkende for å utarbeide gode spørsmål for intervjuene. Vi ønsket å få en forståelse av hvordan IKT-sikkerhetssituasjonen er hos SMB. For å oppnå dette involverte vi eksterne parter. Vi hadde samtaler med oppdragsgiver og andre fagfolk innen IKT-sikkerhet og ved hjelp av deres påstander om hvordan situasjonen er og hypoteser på hvorfor den er slik, utarbeidet vi spørsmål som muliggjorde at vi kunne avdekke interessante funn.

Spørsmålene ble bestående av både refleksjonsspørsmål og kontekstspørsmål. Refleksjonsspørsmål ble formulert slik at de la til rette for refleksjon hos informantene og kontekstspørsmål som stilte konkrete spørsmål om bedriftens praksis med begrenset rom for refleksjon. Vi la vekt på å benytte et forståelig språk under intervjuprosessen for å legge til rette for at informantene, uavhengig av kompetanse, forstod spørsmålene likt.

Vi delte intervjuguiden inn i fire kategorier og ble enige om hva den overordnede hensikten med hver kategori skulle være. Deretter utarbeidet vi spørsmål som bidro til å besvare hensikten. Tabellene under viser hensikten med hver kategori, et sammendrag av spørsmålene og hvilken sammenheng de har med forskningsspørsmålene.

Kategori 0 – IKT-sikkerhet og ansvar	
Hensikt	Å bli kjent med informanten, og samtidig forsikre oss om at vedkommende er godt kvalifisert for å svare på de resterende spørsmålene i intervjuet.
Sammendrag	Kategori 0 inneholder et utvalg oppvarmingsspørsmål der målet er å bli bedre kjent med informanten. Vi ønsker å finne ut av informantens ansiennitet i nåværende stilling og om informanten har overordnet ansvar for IKT-sikkerhet i sin stillingsbeskrivelse. Videre ønsker vi å få i gang en samtale der informanten kan dele sine personlige oppfatninger om hvor stort fokus bedriften har på IKT-sikkerhet. Spørsmålene i denne kategorien kan brukes til å se sammenhenger i øvrige spørsmål basert på informantens stilling, ansvar og oppfatninger.

Tabell 3.1: Beskriver hensikt og et sammendrag av spørsmålene i Kategori 0 - IKT-sikkerhet og ansvar

Kategori 1 – Bedriftenes tilstand	
Hensikt	Få en forståelse av bedriftens tilstand og hvordan de forholder seg til IKT-sikkerhet.
Sammendrag	I kategori 1 vil vi blant annet spørre om hvordan IT-drift er organisert, om de har et strukturert forhold til IKT-sikkerhetsarbeid og om informanten har oversikt over virksomhetskritiske verdier. Et viktig spørsmål i denne kategorien er om virksomheten tjenesteutsetter IT-drift. Bedrifters organisering av IT-drift har betydning for hvordan vi forstår videre besvarelser i intervjuet.

Tabell 3.2: Beskriver hensikt og et sammendrag av spørsmålene i Kategori 1 - Bedriftenes tilstand

Kategori 2 – Etterlevelse av NSMs grunnprinsipper for IKT-sikkerhet, prinsipp 2.9 Etabler evne til gjenoppretting av data	
Hensikt	Besvare forskningsspørsmål 1 ved å utrede bedriftens rutiner og prosesser rundt sikkerhetskopiering, og sammenligne med NSM sine anbefalinger
Sammendrag	Spørsmålene i kategori 2 er avledet fra tiltakene under prinsipp 2.9 Etabler en evne til gjenoppretting av data, og dermed tett knyttet opp med anbefalingene til NSM. Hvert spørsmål undersøker hvorvidt et tiltak er implementert. Ved å stille spørsmål ved tiltakene vil vi kunne måle grad av etterlevelse uavhengig av om informantens bedrift bevisst følger NSMs grunnprinsipper. Informantene sine svar vil dermed gi et godt sammenligningsgrunnlag.

Tabell 3.3: Beskriver hensikt og et sammendrag av spørsmålene i Kategori 2 - Etterlevelse av NSMs grunnprinsipper for IKT-sikkerhet, prinsipp 2.9 Etabler evne til gjenoppretting av data

Kategori 3 – Utfordringer ved etterlevelse	
Hensikt	Besvare forskningsspørsmål 2 som går på hvilke forhold som påvirker etterlevelsen av NSMs anbefalinger.
Sammendrag	For å undersøke hvilke forhold som påvirker etterlevelsen til NSMs anbefalinger, var vi avhengig av å finne ut av hvilke utfordringer SMB møter på i forbindelse med IKT-sikkerhetsarbeid. Gjennom samtaler med oppdragsgiver og andre fagfolk innen IKT-sikkerhet ble det fremlagt følgende utfordringer: - Manglende ledelsesforankring - Økonomi - Begrenset kompetanse/kapasitet Spørsmålene i kategori 3 gir informanten rom til å reflektere rundt disse forholdene, i tillegg til at det stilles spørsmål om det kan være andre forhold.

Tabell 3.4: Beskriver hensikt og et sammendrag av spørsmålene i Kategori 3 - Utfordringer ved etterlevelse

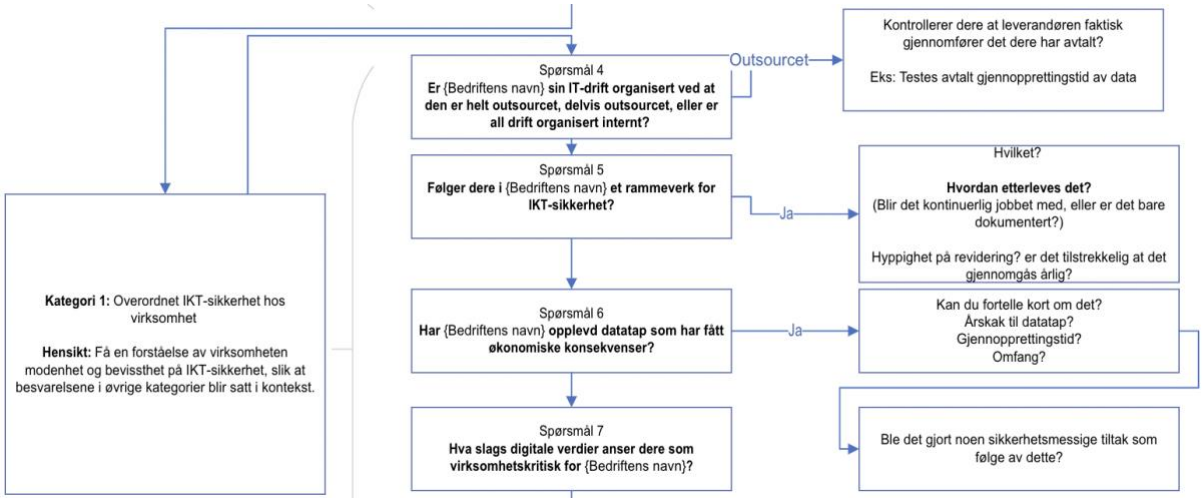
3.3.1 Kvalitetskontroll av intervjuguide

Da vi hadde et endelig utkast, ble intervjuguiden presentert for oppdragsgiver og veileder hvor vi fikk innspill på spørsmålene. Etter at vi var fornøyde med spørsmålene ønsket vi å få et perspektiv fra noen utenfor prosjektet, med den hensikt at de kunne komme med forslag vi ikke hadde tenkt på. Vi gjennomførte derfor et møte med en IKT-sikkerhetsengasjert leder for en virksomhet i Trondheim hvor vi presenterte hva vi ville oppnå med prosjektet og ba om innspill til intervjuguiden. Dette gjorde oss trygge på at spørsmålene var gode og at vi ikke hadde oversett noe essensielt. For fullstendig intervjuguide se: (Vedlegg 2: Intervjuguide).

3.4 Kvalitetssikring av intervjuprosessen

For å teste intervjuguiden utarbeidet vi et flytdiagram (Vedlegg 3: Flytdiagram for intervju) basert på intervjuguiden, som skulle bistå oss i å gjennomføre intervjuene. På grunn av at det kunne være forskjellige oppfølgingsspørsmål, basert på hva intervjukandidatene svarte, ville vi ha en oversiktlig og god måte å gjennomføre dette på.

Ved å benytte dette hjelpemiddelet, forsikret vi oss om at vi kunne holde en flytende og dynamisk samtale. Under slike intervjuer er det ønskelig at informanten kommer med digresjoner og refleksjoner, men da er det viktig styre samtalen tilbake på riktig spor i etterkant. Flytdiagrammet sørget for at vi klarte dette, og hjalp oss med å påse at vi fikk stilt alle spørsmålene fra intervjuguiden.



Figur 3.1: Utdrag fra flytdiagram

Videre ble det gjennomført et testintervju ved hjelp av rollespill, hvor et gruppemedlem tok rollen som leder for en simulert bedrift og de to andre gjennomførte intervjuet på en så realistisk måte som mulig. Dette gjorde at vi fikk testet de digitale verktøyene før intervjuene, i tillegg til at det hjalp oss med å bli trygge på intervjuprosessen og hvordan flytdiagrammet skulle brukes.

3.5 Utvalg av informanter

Utvalget av informanter er viktig for å få resultatene man ønsker i en bacheloroppgave. Ifølge Tjora er «hovedregelen for utvalg i kvalitative intervjustudier at man velger informanter som av ulike grunner vil kunne uttale seg på en reflektert måte om det aktuelle temaet» [1, s. 145]. Derfor ble det mer fokus på å finne informanter som kunne omtale seg reflektert rundt spørsmålene våre, enn informanter som sørget for å gi oss et representativt utvalg fra SMB.

Vi søkte gjennom offentlig tilgjengelig informasjon om bedrifter tilhørende bransjer som oppdragsgiver opplevde var særlig avhengige av å inneha gode rutiner for sikkerhetskopiering. Vi benyttet oss av Brønnøysundregisteret for dette. Deretter kontaktet vi flere av disse bedriftene via e-post. Responsen fra disse bedriftene var lav, og vi fikk ikke tak i noen informanter på denne måten. Derfor var vi nødt til å rekruttere informanter på en annen måte.

På anbefaling fra veileder deltok vi på et møte i Dataforeningens fagstyre for Informasjonssikkerhet. Vi benyttet arenaen for å komme i kontakt med potensielle informanter og eksperter fra bransjen. For å selge inn prosjektet utarbeidet vi et informasjonsskriv (Vedlegg 5: Innsalg av prosjektet). Dette resulterte i at vi kom i kontakt en informant og gjennomførte et møte med en IKT-sikkerhetsekspert. Vi benyttet sistnevnte som en sparringspartner og fikk nyttige tilbakemeldinger på problemstillingen og hans oppfatning av IKT-sikkerhetstilstanden hos SMB.

Gjennom tips fra oppdragsgiver og eget nettverk fikk vi kontakt med et utvalg informanter. En av informantene hjalp oss med å komme i kontakt med andre aktuelle informanter. Denne metoden for å komme i kontakt med interessenter blir ofte beskrevet som snøballmetoden [1, s. 150]. Som et resultat av snøballmetoden tilhørte flere av de informantene vi fikk kontakt med den samme bransjen. Ved rekrutteringen av øvrige informanter la vi vekt på å komme i kontakt med ansatte fra andre bransjer. Bakgrunnen for det var at vi ønsket å få refleksjoner rundt problemet fra forskjellige ståsted. Totalt 11 informanter deltok på dybdeintervjuene.

3.6 Hvordan intervjuene ble gjennomført

I forkant av intervjuene ble informantene tilsendt en modifisert intervjuguide (Vedlegg 2: Intervjuguide) som viste hovedspørsmålene i rekkefølge slik at de kunne forberede seg i forkant av intervjuet. For at det skulle bli lettere for intervjuobjektene å besvare spørsmålene anbefalte vi dem å ha denne tilgjengelig under intervjuene.

Vi benyttet oss av flytdiagrammet (Vedlegg 3: Flytdiagram for intervju) som et hjelpemiddel underveis i intervjuene.

Målet med dybdeintervjuer er ifølge Tjora «i hovedsak å skape en relativt fri samtale som kretser rundt noen spesifikke temaer som forskeren har bestemt på forhånd» [1, s. 127]. Vi ønsket å tilrettelegge for en flytende samtale hvor vi skapte tillitt hos informantene, slik at de følte seg trygge på oss. Derfor hadde vi fokus på å være hyggelige, forståelige og ikke dømmende under samtalene. Det var allikevel viktig at vi var utfordrende og gravende, for å sørge for at vi fikk svar på det vi var ute etter.

I utgangspunktet hadde vi tenkt å gjennomføre intervjuene fysisk, men på grunn av at informantene var såpass spredt geografisk, valgte vi å gjennomføre de fleste digitalt. Siden vi hadde fått godkjent en datahåndteringsplan av Sikt hvor vi kun skulle behandle lydopptak og ikke video, ble vi nødt til å ta lydopptak via nettskjemas diktafon app.

Intervjuene ble gjennomført ved at vi delegerte roller innad i gruppen hvor hvert enkelt gruppemedlem hadde gitte ansvar.

Rolle	**Ansvar**	**Forberedelser**
Intervjuer	- Føre samtalen med intervjuobjektene - Følge flytdiagram - Påse at alle hovedspørsmål besvares	Studere intervjuteknikk *Kapittel 5 Intervjuing i praksis* [1, pp. 159-190] Øve på rollen i praksis
Observatør	- Observere - Notere egne observasjoner og tanker	Lese seg opp på teori og øve på å forklare den på en måte som er tilpasset målgruppen.

	- Stille oppfølgingsspørsmål der det er hensiktsmessig - Forklare teori ved behov	
Moderator	- Observere - Stille oppfølgingsspørsmål der det er hensiktsmessig - Ansvarlig for opptak av lyd - Ansvarlig for å informere intervjukandidater om opptak og hvordan personopplysninger behandles - Holde kontroll på tiden - Styre samtalen tilbake om den sklir for langt fort fra tema	Studere intervjuteknikk *Kapittel 5 Intervjuing i praksis* [1, pp. 159-190] Lese seg opp på sikker datahåndtering, utarbeide datahåndteringsplan og sørge for at den blir fulgt gjennom prosessen

Tabell 3.5: Roller og ansvar ved gjennomføring av intervju

På grunn av at hver rolle medførte at vedkommende måtte forberede seg på forskjellige måter, gikk vi tidlig bort fra å rullere på rollene, da det opplevdes mest effektivt å ha faste roller. Alle tre prosjektmedlemmene deltok i samtlige intervjuer.

3.7 Behandling av materiale fra intervju

På bakgrunn av materialet fra intervjuene sin sensitive natur, var vi nødt til å få godkjenning fra Sikt om behandling av personopplysninger. Vi utarbeidet en databehandlingsplan, et informasjonsskriv (Vedlegg 1: Informasjonsskriv) og en intervjuguide (Vedlegg 2: Intervjuguide). Dette ble vedlagt søknaden som vi fikk godkjent.

Opptak av intervjuene ble gjort med mobilapplikasjonen Nettskjema-diktafon, denne appen er godkjent og anbefalt av NTNU og Sikt [35]. Fra appen blir lydopptaket sendt til Nettskjema som er en sikker nettbasert tjeneste der man kan lagre data [36].

Transkribering av lydopptak ble gjennomført manuelt, da vi ikke kunne garantere at kommersielle tjenester for automatisk transkribering, tilfredsstilte kravene til Sikt for behandling av personopplysninger. Prosessen med transkriberingen startet med at vi spilte av lydopptaket fra nettskjema og transkriberte intervjuet i et dokument som ble lagret i OneDrive. På denne måten sørget vi for at transkriberingen ble lagret separert fra lydopptaket. Under transkriberingen ble personopplysninger anonymisert, slik at det ikke lot seg gjøre å identifisere informanten, dersom man leste transkriberingen.

3.8 Analyse og koding av transkribert intervjumateriale

Vi brukte analyseprogrammet NVivo til å analysere de transkriberte intervjuene. NVivo har en funksjonalitet som heter *koder,* hvor man kan knytte utsagn opp mot bestemte temaer for å se sammenhenger på tvers av filer.

Vi opprettet en kode for hvert spørsmål fra intervjuguiden. Deretter knyttet vi svarene fra informantene opp mot spørsmålet de besvarte. På den måten kunne vi enkelt og på en oversiktlig måte sammenligne svarene. Forholdet mellom koder og utsagn er mange til mange. Det innebefatter at en kode kan ha mange sitater, og et sitat kan kobles opp mot flere koder.

Siden vi i intervjuene la til rette for digresjoner og refleksjoner rundt spørsmålene, var det ikke alt som kunne kodes direkte til spørsmål fra intervjuguiden. I denne sammenhengen opprettet vi andre koder. Et eksempel på en slik kode var *interessante utsagn*, vist under.

Figur 3.2: Skjermbilde fra NVivo som viser et eksempel av koden: interessante utsagn

3.8.1 Metode brukt for å måle etterlevelse av prinsipp 2.9

For å kunne si noe om til hvilken grad de ulike bedriftene etterlever prinsipp 2.9 i NSMs grunnprinsipper for IKT-sikkerhet, så utviklet vi metrikker som gjorde at vi kunne tallfeste etterlevelsen av grunnprinsippene. Metrikkene vi har valgt å tallfeste er de ulike tiltakene som inngår i grunnprinsippet.

Vi valgte å vektlegge de forskjellige tiltakene forskjellig, basert på prioritetsgruppen deres. Fullstendig etterlevelse av anbefaling i prioritetsgruppe 1 gir 20 poeng, prioritetsgruppe 2 gir 10 poeng og prioritetsgruppe 3 gir 5 poeng.

Totalt 40 poeng var mulig å oppnå og grad av etterlevelse ble vurdert på følgende skala:

Høy etterlevelse	Middels etterlevelse	Lav etterlevelse
31-40 poeng	11-30 poeng	0-10 poeng

Tabell 3.6: Skala som kobler poengsum mot grad av etterlevelse

Vurderingen av hver enkelt informants etterlevelse av prinsipp 2.9 er vedlagt (Vedlegg 4: Informantenes etterlevelse av prinsipp 2.9). Hva vi har vurdert og begrunnelse for hvordan vi har vektlagt metrikkene forklares i *Tabell* 3.7.

Tilhørende tiltak	Metrikk	Vektlagt	Begrunnelse av vektlegging
2.9.1	Har en plan for sikkerhetskopi	0/4	Dette punktet er i prioritetsgruppe 1 og vil derfor kunne gi maksimalt 20 poeng. Hvis en bedrift har en nedskrevet plan for sikkerhetskopiering, vil de få 4 poeng. NSM beskriver punkter som skal inngå i planen, og for hvert av disse punktene som inngår i bedriftens plan vil de få 2 poeng.
	Antall punkter beskrevet i plan for sikkerhetskopi	0-16	
2.9.2	Sikkerhetskopi av programvare	0/5	Dette er prioritetsgruppe 3 og vil derfor gi maksimalt 5 poeng. NSM beskriver et minimum av hva som skal inkluderes ved sikkerhetskopiering av programvare. Om bedriften inkluderer dette minimumet i sin sikkerhetskopiering vil de få full uttelling her. Om de ikke inkluderer minimumet eller informanten ikke har oversikt over om bedriften tar sikkerhetskopi av programvare, vil de få 0 poeng.
2.9.3	Testes gjenoppretting regelmessig	0/10	Dette er prioriteringsgruppe 2 og vil derfor gi maksimalt 10 poeng. Her vil bedriften bli tildelt 10 poeng om de intensjonelt tester gjenoppretting av sikkerhetskopiene sine regelmessig. Dersom bedriften ikke gjør dette vil de få 0 poeng, til tross for at de kanskje kan ha gjenopprettet filer tidligere.
2.9.4	Oversikt over beskyttelse av sikkerhetskopi	0-1	Dette er prioriteringsgruppe 3 og vil derfor gi maksimalt 5 poeng. Her vil bedriften få 1 poeng om informanten har oversikt over hvordan sikkerhetskopiene deres beskyttes. NSM beskriver 4 tiltak for å beskytte sikkerhetskopiene. For hvert av disse punktene som informanten vet at de gjennomfører vil de få 1 poeng. Dersom informanten ikke vet hvordan sikkerhetskopiene beskyttes vil de få 0 poeng her.
	Antall punkter tilfredsstilt	0-4	

Tabell 3.7: Oversikt over metrikker for å måle etterlevelse av prinsipp 2.9

3.9 Utarbeiding av oppfølgingsundersøkelse

Omtrent en måned etter at intervjuene ble gjennomført, sendte vi ut en spørreundersøkelse til informantene. Bakgrunnen for at vi valgte å følge opp informantene, var at vi ønsket å se om intervjuene hadde hatt noen påvirkning, og om informantene hadde gjort noen tiltak for å bedre bedriftens IKT-sikkerhet i ettertid.

Hensikten med oppfølgingsundersøkelsen var ikke å finne ut av hvilken bedrift som hadde gjort hvilke tiltak, men heller generelt hvilken påvirkning intervjuene hadde på informantene. Dermed kunne vi gjøre undersøkelsen helt anonym uten noen personopplysninger, og vi trengte ikke godkjenning fra Sikt i forkant.

Id	Spørsmålstype	Spørsmål	Hensikt
1	Flervalg	Hadde du hørt om NSMs grunnprinsipper i forkant av intervjuet?	Vi ønsket å få svar fra alle informantene på dette spørsmålet. Da vi glemte å stille spørsmålet til samtlige under intervjuene, inkluderte vi det i spørreskjemaet.
2	Flervalg	Har du sett på NSM-grunnprinsipper etter at vi hadde intervju med deg?	Se om intervjuet førte til at informanten ble interessert i NSMs grunnprinsipper.
3	Flervalg	Har dere tenkt til å ta i bruk et rammeverk for IKT-sikkerhet etter vi har hatt intervju med deg?	Finne ut om intervjuet førte til at informanten innså nytten av å følge et rammeverk for IKT-sikkerhet.
3.1	Flervalg *Dersom «ja» på spørsmål 3*	Tenker du å benytte NSMs grunnprinsipper som hjelpemiddel?	Se om vi klarte å få informantene til å benytte NSMs grunnprinsipper.
4	Flervalg	Dersom dere tjenesteutsetter (*outsourcer*) IT-drift, har dere gjennomført leverandørkontroll i etterkant av intervjuet?	Ingen av informantene gjennomførte leverandørkontroll, men mange sa at dette var noe de skulle ta tak i. Vi ønsker her å se om det ble gjennomført.
4.1	Flervalg *Dersom informanten svarer noe annet enn «tjenesteutsetter ikke IT-drift» på spørsmål 4*	*Har dere gjennomgått kontrakt med IT-leverandøren deres etter vi hadde intervju med deg?*	Se om intervjuet førte til at informantene som tjenesteutsatte IT-drift, innså viktigheten av å ha kontroll på hva de har avtalt med sin IKT-driftsleverandør. Og undersøke om de gjorde konkrete tiltak.
5	Fritekst	Kan du utdype litt dersom dere har gjort noen endringer i deres sikkerhetskopieringspraksis i etterkant av intervjuet?	Se om intervjuet førte til en forbedring av bedriftens IKT-sikkerhet.

6	Fritekst	Har dere snakket mer om IKT-sikkerhet i etterkant av intervjuet?	Se om intervjuet førte til økt fokus på IKT-sikkerhet.
7	Fritekst	Førte intervjuet til noe annet, som ikke er nevnt i spørsmålene over?	Se om intervjuet førte til noe som ikke ble spurt om i undersøkelsen.

Tabell 3.8: Spørsmål og hensikt fra oppfølgingsundersøkelse

4 Resultater

4.1 Introduksjon

I resultatkapittelet presenterer vi funnene fra intervjuene med informantene. Vi har strukturert kapittelet etter kategoriene i intervjuguiden. For hver kategori vil hensikten bli beskrevet, og for de kategoriene som har en tydelig sammenheng med forskningsspørsmålene vil dette bli spesifisert. Vi fokuserer på å gi et helhetsinntrykk av informantene, men ved noen anledninger vil det være særlige funn som gjør at vi legger vekt enkelte informanters besvarelser. Avslutningsvis vil vi presentere resultatene fra oppfølgingsundersøkelsen.

4.2 Kategori 0: IKT-sikkerhet og ansvar

I kategori 0 er hensikten å bli kjent med informantene, i tillegg til å forsikre oss om at de er godt egnet til å besvare spørsmålene. Svarene fra kategori 0 skal også brukes som kontekst for informantenes øvrige besvarelser.

Informantene vil bli referert til etter stillingen de i innehar i bedriften.

Informantene
Arkitekt 1
Arkitekt 2
CCO
CISO
CTO
Daglig leder
IT-sjef
Landskapsarkitekt 1
Landskapsarkitekt 2
Sivilarkitekt
Partner

Tabell 4.1: Informantene

Ansvar for IKT-sikkerhet

Selv om alle informantene har et overordnet ansvar for IKT-sikkerhet i bedriften, så er det ikke alle som har dette ansvaret nedskrevet i sin stillingsbeskrivelse. Årsaken til at de fikk ansvar for IKT-sikkerhet varierer mellom egeninteresse for IKT, kompetanse og tilfeldigheter.

Tabell 4.2 viser informantene som har ansvar for IKT-sikkerhet spesifisert i stillingsbeskrivelsen og hvorvidt de har relevant utdannelse til å gjenspeile ansvaret.

Informant	Ansvar for IKT-sikkerhet i stillingsbeskrivelsen?	IT-relatert utdannelse
CISO	Ja	Ja
IT-sjef	Ja	Ja
CTO	Ja	Nei
Landskapsarkitekt 1	Ja	Nei
Landskapsarkitekt 2	Ja	Nei

Tabell 4.2: Informantene som har ansvar for IKT-sikkerhet spesifisert i stillingsbeskrivelsen

Øvrige informanter har verken ansvar for IKT-sikkerhet i stillingsbeskrivelsen eller utdanning innen IT. Disse informantene begrunner årsaken til at de har fått ansvar for IKT-sikkerhet slik:

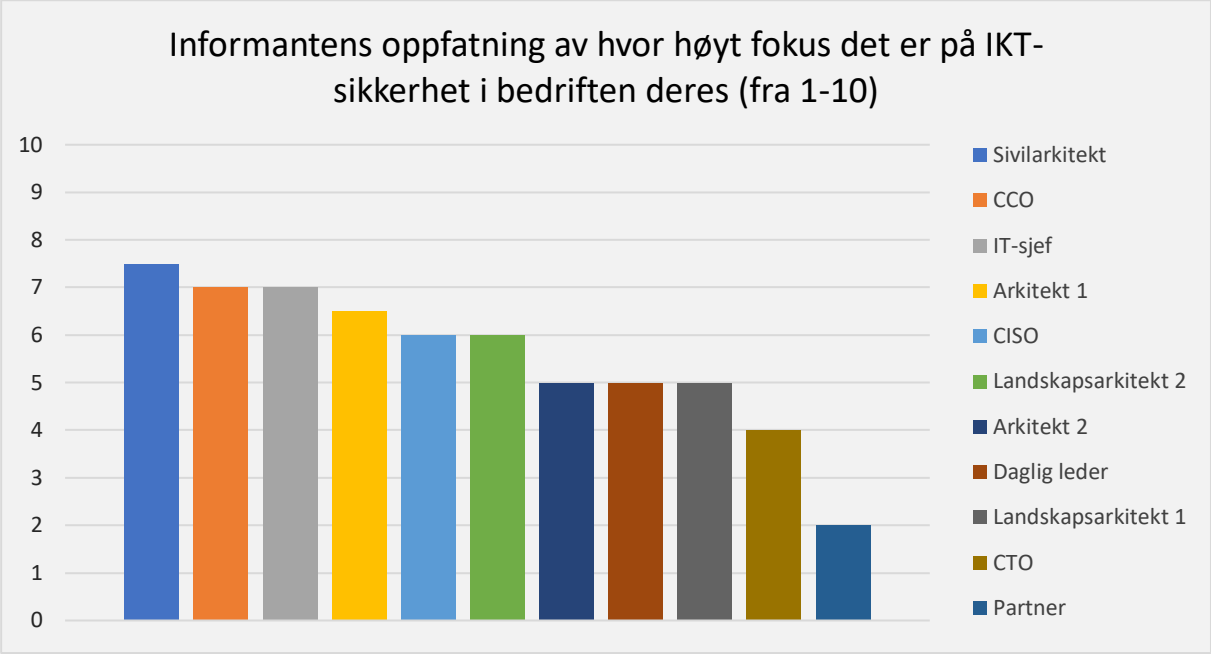
CCO - Bedriften informanten jobber for har ikke så streng stillingsbeskrivelse, men informanten opplyser om at det ikke er noe tvil om at det er vedkommende sitt ansvar. Informanten har tidligere erfaring innenfor teknologibransjen.

Arkitekt 1 - Informanten opplyser å ha: «marginal erfaring med data fra tidligere jobb».

Sivilarkitekt, Daglig leder, Arkitekt 2 og Partner - Disse informantene oppgir at det var noe tilfeldig at ansvaret for IKT-sikkerheten i bedriften ble tilegnet dem. Sivilarkitekten sier eksplisitt at hen ikke er så interessert i IT og data, mens arkitekt 2 understreker at hen mangler dedikasjon og kunnskap til IT. Når vi spør Partneren om det er hen som jobber med IKT-sikkerhet i bedriften så sier han følgende: «Det er ingen som ordner med IKT-sikkerhet, men det er i hvert fall ikke jeg».

Fokus på IKT-sikkerhet

Vi var ute etter informantenes subjektive mening om hvor stort fokus det er på IKT-sikkerhet i bedriften. Dette kan si noe om bedriftenes modenhet og bevissthet på IKT-sikkerhet. Hensikten med spørsmålet var finne ut hva de selv mener, slik at vi senere kunne sammenligne deres svar med vår oppfattelse av IKT-sikkerhet i bedriftene. Holdbarheten av disse resultatene diskuteres i avsnitt *5.5 Forskningens troverdighet*.



Figur 4.1: Informantens oppfatning av hvor høyt fokus det er på IKT-sikkerhet i bedriften deres

Det var vesentlige forskjeller i hvor stort fokus informantene opplevde at det var på IKT-sikkerhet i bedriften deres. Under har vi trukket frem begrunnelsen noen av informantene legger til grunn for vurderingen.

Partner (Fokus: 2) - Dette var informanten som behøvde kortest betenkningstid for å besvare spørsmålet. Informanten begrunner sin vurdering med at de snakker mye om IKT-sikkerhet, men at det stopper der.

CTO (Fokus: 4) - Informanten vet at de har lavt fokus og nevner flere årsaker til det. Informanten begrunner vurderingen med manglende kompetanse og at de er en relativt nyoppstartet bedrift som ikke har fått alt på plass enda. Videre sier informanten at de ønsker å ligge på rundt 7 på skalaen etter hvert.

CISO (Fokus: 6) - Informanten sier: «Jeg skulle likt og sagt at det var 10, men jeg tenker på at vi er på rundt 6». Årsaken til det er at mange av de øvrige ansatte er velig lite bevisst på IKT-sikkerhet. Bedriften har en del utviklere ansatt, og sier at det skorter på sikkerhet både i deres leveranser, og på enkle ting som å låse PC-en når de forlater den. Informanten har et ønske om å være oppe på 8 på skalaen i løpet av året, og har en plan om å gjennomføre IKT-sikkerhetsopplæring av alle ansatte for å oppnå dette.

Landskapsarkitekt 2 (Fokus: 6) - Informanten mener at fokuset ligger på 6, men at IKT-sikkerhet ikke er noe de snakker eller tenker så mye på i bedriften.

CCO (Fokus: 7) - Informanten har tidligere hatt et ansettelsesforhold i en virksomhet hvor IKT-sikkerhet sto høyt på radaren. Informanten sammenligner denne erfaringen med hvordan han opplever fokus på IKT-sikkerhet i nåværende bedrift. Grunnet at nåværende bedrift er mindre og risikoen for IKT-sikkerhetshendelser er litt lavere, er det nå ikke behov for like stort fokus på IKT-sikkerhet.

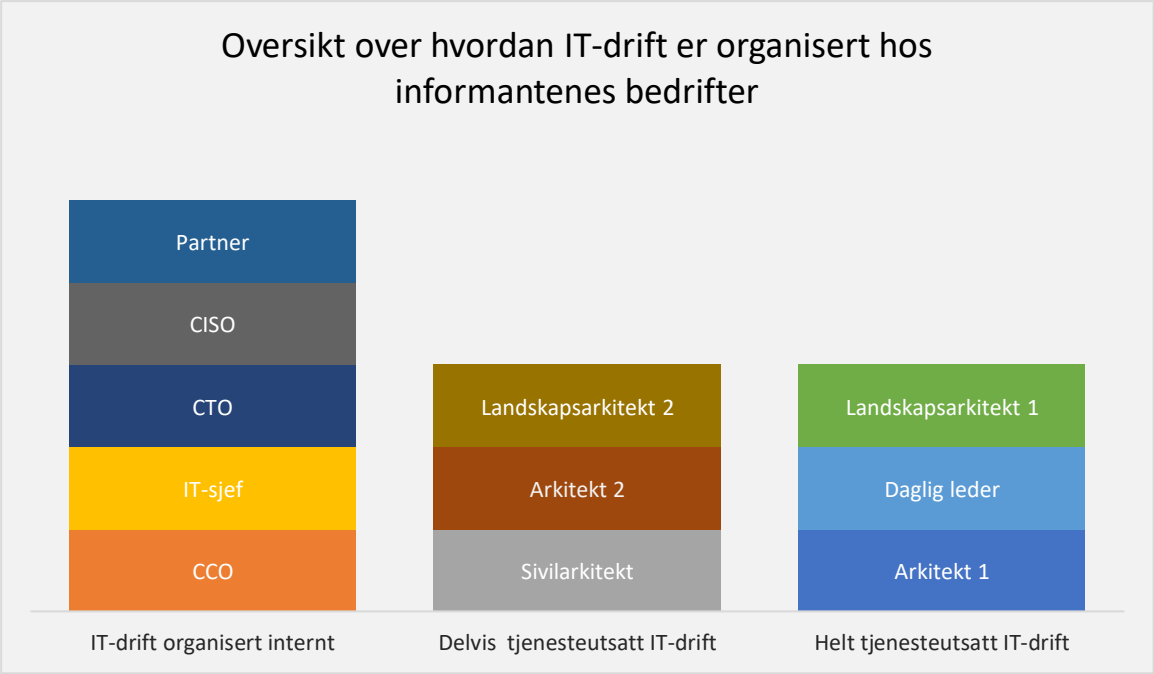
Sivilarkitekt (Fokus: 7,5) - Informanten begrunner stort fokus med at han selv alltid tenker på IKT-sikkerhet, og spesielt sikkerhet når det kommer til sikkerhetskopiering da det er meget kritisk dersom de skulle miste data.

4.3 Kategori 1: Bedriftenes tilstand

I kategori 1 er hensikten å få en forståelse av bedriftens tilstand og hvordan de forholder seg til IKT-sikkerhet. Informantenes svar fra kategori 1 kan også brukes som kontekst for deres øvrige besvarelser.

Tjenesteutsetting

Alle informantene ble spurt om deres IT-drift er organisert ved at den er helt tjenesteutsatt, delvis tjenesteutsatt, eller om all drift er organisert internt. Bedrifters organisering av IT-drift har påvirkning på hvordan vi forholder oss til og tolker øvrige besvarelser i intervjuet. *Figur* 4.2 viser en oversikt over hvordan IT-drift er organisert hos de forskjellige informantenes bedrifter.



Figur 4.2: Oversikt over hvordan IT-drift er organisert hos informantenes bedrifter

Som vi kan se er IT-driften til omtrent halvparten av informantene organisert ved at den i en grad er tjenesteutsatt. Felles for alle som helt eller delvis tjenesteutsetter IT-drift er at de tilhører arkitektbransjen.

2 av informantene som tjenesteutsetter deler av driften har valgt å ta drifte sikkerhetskopiering selv. *Figur* 4.3 viser en oversikt over hvilke bedrifter som gjennomfører sikkerhetskopiering selv.

Figur 4.3: Diagram som viser hvilke bedrifter som gjennomfører sikkerhetskopiering selv

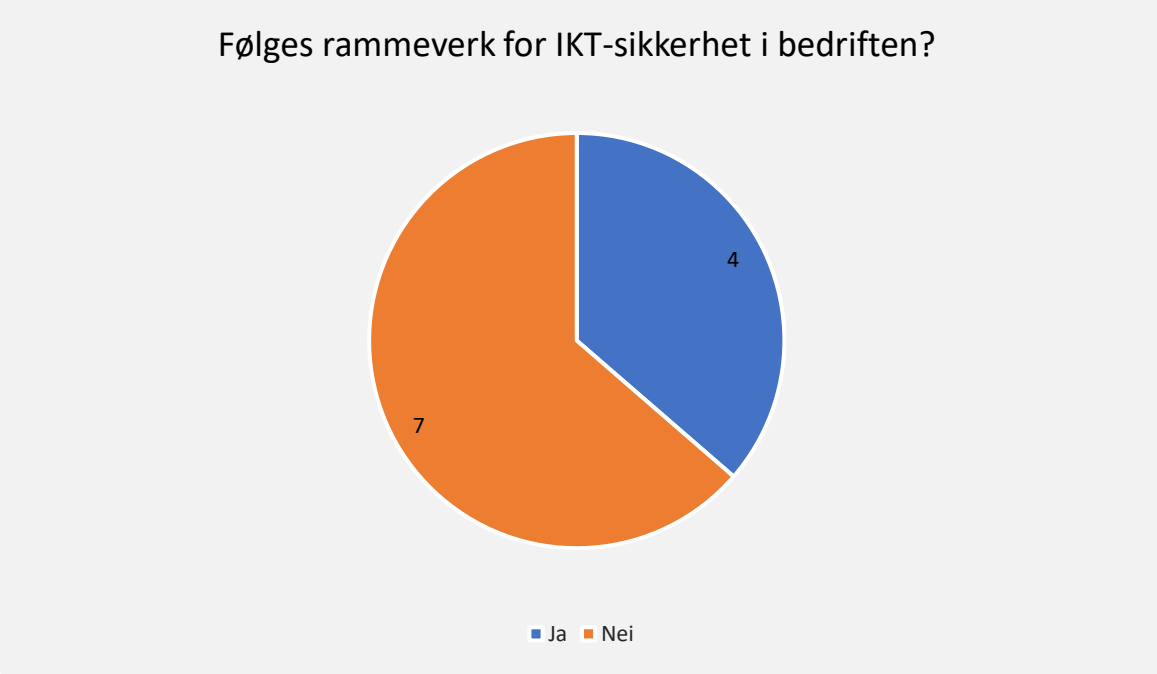
Leverandørkontroll

De som enten helt eller delvis hadde tjenesteutsatt IT-drift fikk spørsmål om de gjennomfører noen form for leverandørkontroll. Her svarte samtlige 6 informanter at de aldri har kontrollert sin IKT-driftsleverandør, utover at det ved enkeltfiler har blitt gjenopprettet ved behov.

Bruk av rammeverk for IKT-sikkerhet

Alle informantene ble spurt om de følger et rammeverk for IKT-sikkerhet. Siden det kan være litt uklart hva definisjonen av et rammeverk for IKT-sikkerhet er, ba flere av informantene oss definere hva vi mente med det. Vi la vår definisjon til grunne og eksemplifiserte med å beskrive NSMs grunnprinsipper. På denne måten fikk alle informantene lik oppfatning av hva vi la i et rammeverk for IKT-sikkerhet.

Figur 4.4 viser hvor mange av bedriftene som følger et rammeverk for IKT-sikkerhet:



Figur 4.4: Diagram som viser antall informanter som følger et rammeverk for IKT-sikkerhet

Et rammeverk for IKT-sikkerhet følges ikke av flertallet av bedriftene vi intervjuet. Arkitekt 2 opplyser om at de følger et rammeverk for IKT-sikkerhet, men gjennom dialog viser det seg at det er et kvalitetssikringssystem som ikke inneholder noen tiltak relatert til IKT-sikkerhet. 1 av informantene opplyste om at deres IKT-driftsleverandør har ISO-sertifisering, men husket ikke akkurat hvilken type.

Av 11 informanter fulgte 4 et rammeverk for IKT-sikkerhet. Under utdyper vi hva slags rammeverk bedriftene følger.

Sivilarkitekt - Informanten opplyste om at bedriften følger et rammeverk som de har utviklet selv. Revisjon og gjennomgang av rammeverket gjennomføres årlig. Informanten opplyser om at rammeverket inneholder rutiner for arkivering, intern organisering og roller innad, hensyn til GDPR og sikkerhetsrutiner for ansatte.

IT-sjef - Informanten opplyser om at bedriften benytter seg av ISO27001. De er ikke sertifisert etter denne internasjonale standarden, men bruker den som en støttemur i sikkerhetsarbeidet sitt. Videre oppgir informanten at de benytter seg av NSMs grunnprinsipper for IKT-sikkerhet som et tillegg.

CISO - Bruker NSMs grunnprinsipper for IKT-sikkerhet som en integrert del av arbeidsflyten i bedriften.

CCO - Informanten forteller at de følger deler av et rammeverk fra en tidligere bedrift som informanten jobbet hos.

Har virksomheten opplevd datatap som fikk økonomiske konsekvenser?

Vi ville se på hvordan virksomheter som hadde opplevd datatap med økonomiske konsekvenser forholdte seg til sikkerhetskopiering. Innfører bedriftene som opplever datatap tiltak i etterkant for å bedre IKT-sikkerheten sin? Er det slik at de bedriftene som har opplevd datatap nå er bedre rustet mot det enn de øvrige bedriftene vi intervjuer?

Det var totalt 4 informanter som oppga at de hadde opplevd datatap med økonomiske konsekvenser. Under utdyper vi deres erfaringer.

Arkitekt 1 - Bedriften har opplevd å bli infisert av løsepengevirus, som inntraff ved at en ansatt trykket på en lenke i en e-post. De hadde gode rutiner på sikkerhetskopiering og beskyttelse av sikkerhetskopiene, dermed ble ikke konsekvensen større enn at de tapte omtrent en halv arbeidsdag. Bedriften var fornøyd med IKT-sikkerheten og innførte ikke noen ytterligere sikkerhetstiltak etter hendelsen. Informanten opplevde at ledelsen ble mer bevisst på IKT-sikkerhet og alvorligheten av slike sikkerhetshendelser.

Selv om det ikke ble innført noen konkrete tiltak, så førte hendelsen til at ledelsen innså hvor alvorlig det kunne blitt. IKT-sikkerhet ble ytterligere forankret ved at de ansatte ble bevisstgjort på trusselen ved å klikke på lenker.

Arkitekt 2 - Bedriften har delvis tjenesteutsatt IT-drift, og har valgt å drifte sikkerhetskopiering selv. Informanten opplyser om at bedriften ikke har opplevd datatap som har fått økonomiske konsekvenser, men gjennom videre dialog kommer det frem at det hender at de mister en sikkerhetskopi, eller at de mister noen filer. Dette skjer i forbindelse ved at de som har ansvar for sikkerhetskopiering ikke har vært på jobb, og dermed har de ikke tatt sikkerhetskopi fra dagen før. Informanten konkluderer med at de har tapt tid som kunne vært brukt på verdiskapende aktiviteter, da de har måttet gjøre arbeidet på nytt. Det har ikke blitt innført noen risikoreduserende tiltak i etterkant av disse hendelsene.

Landskapsarkitekt 2 - Informanten opplevde at en filserver krasjet. Dette førte til flere dager med nedetid da de måtte gjenopprette fra sikkerhetskopien. Informanten mener at nedetiden medførte at bedriften tapte «en god del penger».

Bedriften har også opplevd datatap i mindre skala, slik som utilsiktet sletting av filer. Dette har ført til at de har måttet bruke en del tid på å finne ut hva som har skjedd, før de kunne gjenopprette fra sikkerhetskopi. Informanten blir stilt spørsmål til hva som er den vanligste årsaken til at slike hendelser forekommer. Informanten svarer at brukerfeil er årsaken, men det kommer for øvrig frem at ansatte har for høye tilgangsrettigheter og dermed har mulighet til å slette filer som i utgangspunktet ikke bør bli slettet. Underveis i intervjuet går det opp for informanten at bedriften ikke har god nok tilgangskontroll på filservere.

Partner - Informanten sier at «i likhet med alle andre har vi også mistet dokumenter, men ikke i en slik skala at vi har kunnet tallfeste det». Bedriften opplevde en hendelse som ikke var relatert direkte til sikkerhetskopiering, men som påførte deres kunde et tap på rundt 10 millioner, i tillegg til at de ikke kunne fakturere for oppdraget som hadde en verdi på over hundre tusen. Dersom de hadde fått krav på kundens tap opplyser informanten at hendelsen trolig ville medført en konkurs for bedriften. Selv om denne hendelsen ikke var direkte relatert til datatap, så var det en skremmende opplevelse som førte til at informanten innså verdien av *forebyggende IKT-sikkerhetsarbeid*. Til tross for dette ble det ikke innført noen tiltak, og IKT-sikkerhetsarbeid utføres fortsatt *ad-hoc* når det oppstår problemer.

Virksomhetskritiske verdier

Informantene ble bedt om å identifisere hvilke digitale verdier de anså som kritiske for bedriften. Formålet med dette spørsmålet var å sikre at informantene kunne svare på etterfølgende spørsmål, som omhandlet en vurdering av de økonomiske konsekvensene, dersom disse verdiene midlertidig eller permanent ble utilgjengelige.

Svarene vi får fra informantene er gjennomgående like. Alle informantene gir konkrete svar på hvilke digitale verdier som er virksomhetskritisk for dem. Noen av informantene har kartlagt verdiene, mens andre har god nok oversikt over bedriften til å tenke seg fram til hvilke verdier som er mest virksomhetskritisk. 2 av informantene har anslått kostnad ved tap av disse verdiene. Ytterligere 4 informanter kommer med omtrentlige tall på hva de tenker seg det vil koste, og noen spesifiserer hvor mange dager bedriften kan overleve uten tilgang til virksomhetskritisk data.

Et avvik er at en informant oppgir at de ikke tør å anslå kostnaden ved datatap. Informanten sier at de har så lav IKT-sikkerhet, at om de setter seg ned for å tenke på farene ved at noe kan gå galt, så ville de blitt handlingslammet.

4.4 Kategori 2: Etterlevelse av NSMs grunnprinsipper for IKT-sikkerhet, *prinsipp* 2.9 Etabler evne til gjenoppretting av data

I denne kategorien er hensikten å besvare forskningsspørsmål 1 som går på bedriftens rutiner og prosesser rundt sikkerhetskopiering sammenlignet med NSM sine anbefalinger. Spørsmålene er avledet fra tiltakene under prinsipp 2.9, og dermed tett knyttet opp med anbefalingene til NSM. Informantene sine svar vil dermed gi et godt sammenligningsgrunnlag.

Av de 11 informantene vi har intervjuet oppgir 4 at de følger et rammeverk for IKT-sikkerhet. Det er flere likhetstrekk mellom rammeverk for IKT-sikkerhet, da mange er tett knyttet opp mot ISO/IEC 27002. Det er dermed mulig å etterleve NSM sine grunnprinsipper for IKT-sikkerhet, selv om man følger et annet rammeverk eller beste praksiser innen informasjonssikkerhet.

Har bedriften en plan for sikkerhetskopiering – tiltak 2.9.1

Flere av informantene var usikre på hva som defineres som en plan, og stilte spørsmål ved dette. Vi valgte å presisere at spørsmålet gikk på hvorvidt de hadde en dokumentert plan. Årsaken til det, var at flere svarte ja, selv om rutinene og prosessene for sikkerhetskopiering i stor grad viste seg å være *ad-hoc*-løsninger. *Figur* 4.5 viser antall informanter som har en dokumentert plan for sikkerhetskopiering av alle virksomhetsdata.

Figur 4.5: Diagram over antall informanter som har en dokumentert plan for sikkerhetskopiering av alle virksomhetsdata

Tiltak 2.9.1 som går på å ha en plan for sikkerhetskopiering av all virksomhetsdata inngår i NSM sin prioriteringsgruppe 1. Til tross for at tiltaket er svært kostnadseffektivt og gir høy sikkerhetsmessig effekt, er det kun 6 informanter som etterlever det.

De informantene som hadde en dokumentert plan for sikkerhetskopiering, ble stilt oppfølgingsspørsmål rundt omfanget av planen. Oppfølgingsspørsmålene gikk på hvorvidt planen til virksomheten inneholdt de 8 punktene NSM anser som et minimumskrav av hva en plan for sikkerhetskopiering bør beskrive. *Figur* 4.6 viser antall punkter beskrevet i informantenes plan for sikkerhetskopiering.

Figur 4.6: Diagram som viser antall punkter beskrevet i plan for sikkerhetskopiering

Felles for alle som har en plan for sikkerhetskopiering er at den beskriver hvilke data som skal sikkerhetskopiers samt oppbevaringstiden for sikkerhetskopiene. Kun én informant oppgir at planen beskriver alle punktene NSM anser som et minimumskrav og et fellestrekk for resterende virksomheter er at deres plan ikke beskriver prosedyrer for feilet sikkerhetskopiering, samt regelmessighet på sikkerhetskopiering basert på dataens verdi.

Daglig Leder – Informanten oppgir at planen er en del av et internt kvalitetssikringssystem i bedriften. Her beskrives det hvordan dataen skal behandles og hvordan sikkerhetskopiering skal foregå.

IT-sjef - Informanten presiserer at de har en plan, men at den ikke er skrevet ned som en fin guide.

Landskapsarkitekt 1 - Informanten forteller at de har en plan, men at denne planen er utarbeidet av IKT-sikkerhetsleverandør. De har mottatt planen fra leverandør, men ikke satt seg godt inn i den.

Arkitekt 1 - Informanten forteller at de har en plan for sikkerhetskopiering. Denne planen omfatter ikke all virksomhetsdata, men kun data som de mener er virksomhetskritisk.

CISO - Informanten virker å ha en god og strukturert plan, som beskriver alle punktene NSM anbefaler.

Tas det sikkerhetskopi av programvare? - tiltak 2.9.2

Også på dette spørsmålet var det behov for å presisere hva som inngår i programvare. De fleste informantene svarte i utgangspunktet nei, men gjennom samtaler kom det fram at mange inkluderte maler for virtuelle maskiner, skyinfrastruktur eller konfigurasjon i sine sikkerhetskopier. *Figur* 4.7 viser antall bedrifter som inkluderer programvare i sine sikkerhetskopier.

Figur 4.7: Diagram som viser hvor mange av bedriftene som inkluderer programvare i sine sikkerhetskopier

Arkitekt 1 - Sikkerhetskopi av programvare er begrenset til Sikkerhetskonfigurasjon. De tar ikke sikkerhetskopi av annen programvare grunnet at det er tilgjengelig via skytjenester.

Sivilarkitekt - Informanten mener at dette ikke er relevant for sin bedrift og sier at det er raskere å laste ned programvare fra internett, derfor er det utelatt fra sikkerhetskopieringspraksis.

Daglig Leder - Informanten vet ikke omfanget av bedriftens sikkerhetskopieringspraksis. Informanten stoler i høy grad på at IKT-driftsleverandør inkluderer det som er nødvendig i sikkerhetskopiene.

Landskapsarkitekt 1 – Informanten forteller at de hadde avtale om sikkerhetskopiering av programvare med sin tidligere IKT-driftsleverandør, men at det nå er utelatt på grunn av stor datamengde. I tillegg er mye av programvaren de bruker enkel å laste ned fra internett. Selv om det meste er utelatt har de likevel sikkerhetskopi av serverbilder som en del av praksisen.

Arkitekt 2 – Informanten forteller at de ikke har behov for sikkerhetskopiering av programvare, grunnet at alt er nettbasert. Informanten er usikker på om konfigurasjonene til deres interne IKT-system sikkerhetskopieres, da det er IKT-driftsleverandør som har ansvaret for det.

Partner – Informanten oppgir at bedriften har en egenutviklet programvare der de har ulike servere som er dedikert til produksjon, testing og staging. Dette kan fungere som en sikkerhetskopi i visse tilfeller, som for eksempel hvis produksjon-serveren går ned. De har derimot ikke noen sikkerhetskopi av infrastrukturen som brukes til programvaren.

Testes gjenoppretting regelmessig? - tiltak 2.9.3

På spørsmål om bedriftene regelmessig tester gjenoppretting, var det flere informanter som misforsto spørsmålet og svarte ja. Etter at vi presiserte at spørsmålet var om det ble testet regelmessig endret svarene seg og samtlige informanter svarte nei. Av de som har gjennomført gjenoppretting av filer fra sikkerhetskopi, er dette kun blitt gjort ved behov.

IT-sjef - Informanten svarer at de ikke har utført dette i full skala, men delvis. De har ingen plan på hvor ofte det utføres og har ikke utført en total gjenoppretting av hele miljøet.

Daglig leder - På spørsmål om hvorfor dette ikke blir gjort svarer informanten: «Vi er ikke bevisste rett og slett».

Landskapsarkitekt 1 - Informanten opplyser om at de har byttet IKT-driftsleverandør for fire måneder siden. I prosessen med å bytte leverandør opplevde informanten at den nye leverandøren var svært kompetent på feltet og at IKT-sikkerheten ville bli tatt godt hensyn til. Det ble blant annet avtalt at det skulle gjennomføres gjenopprettingstester av sikkerhetskopi, men dette har ikke blitt utført enda. Informanten opplever at den nye leverandøren ikke har levd helt opp til forventningene, og uttrykker usikkerhet knyttet til hvor god leverandøren egentlig er.

Arkitekt 2 - På spørsmål om hva som er årsaken til at dette ikke blir gjort regelmessig svarer informanten: «det er fordi vi stoler på sikkerhetskopien, så vi har ikke sett behov for å teste det».

Beskytt sikkerhetskopier mot tilsiktet og utilsiktet sletting, manipulering og avlesning - tiltak 2.9.4

Flere av informantene manglet kompetanse og/eller oversikt til å gi svar på hvilke tekniske løsninger de brukte for beskyttelse av sikkerhetskopiene. Det vi derimot fikk gode svar på var hvor god oversikt informantene hadde over beskyttelsen av sikkerhetskopiene. Tabellene under viser vår oppfatning av hvor god oversikt informantene hadde over beskyttelse av sikkerhetskopiene sammenstilt med hvordan IT-driften er organisert.

God oversikt over beskyttelse av sikkerhetskopi	
CISO	Intern IT-drift
IT-sjef	Intern IT-drift
CTO	Intern IT-drift
CCO	Intern IT-drift

Tabell 4.3: Informantene som har god oversikt over hvordan sikkerhetskopiene beskyttes.

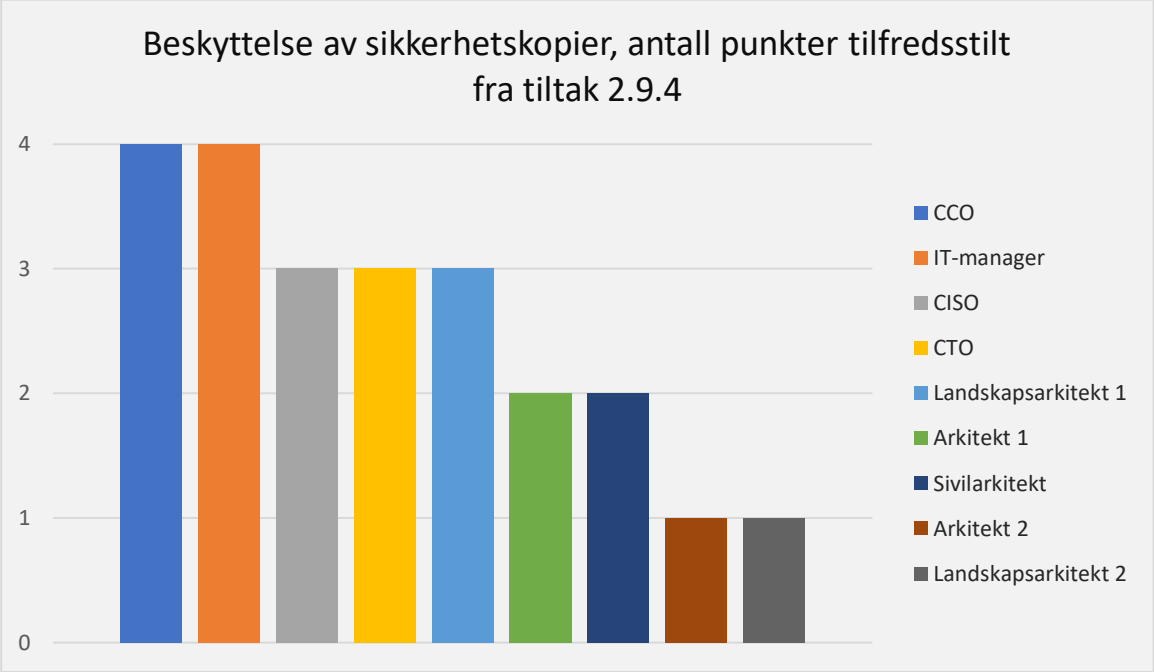
Delvis oversikt over beskyttelse av sikkerhetskopi	
Sivilarkitekt	Delvis outsourcet IT-drift
Landskapsarkitekt 2	Delvis outsourcet IT-drift
Arkitekt 2	Delvis outsourcet IT-drift
Landskapsarkitekt 1	Helt outsourcet IT-drift
Arkitekt 1	Helt outsourcet IT-drift

Tabell 4.4: Informantene som har delvis oversikt over hvordan sikkerhetskopiene beskyttes.

Liten/ingen oversikt over beskyttelse av sikkerhetskopi	
Daglig leder	Helt outsourcet IT-drift
Partner	Intern IT-drift

Tabell 4.5: Informantene som har liten/ingen oversikt over hvordan sikkerhetskopiene beskyttes.

I tiltak 2.9.4 trekker NSM frem 4 punkter som de anbefaler for beskyttelse av sikkerhetskopier mot tilsiktet og utilsiktet sletting, manipulering og avlesning. Figur 4.8 viser en oversikt over hvor mange av disse punktene som informantene tilfredsstiller.



Figur 4.8: Diagram som viser antall punkter informantene har tilfredsstilt fra tiltak 2.9.4.

Partner og Daglig leder - Informantene hadde liten/ingen oversikt over hvordan sikkerhetskopiene beskyttes og er dermed ikke vist i dette diagrammet.

4.5 Kategori 3: Utfordringer ved etterlevelse

I denne kategorien er hensikten å besvare forskningsspørsmål 2 som går på hvilke forhold som påvirker etterlevelsen av NSMs anbefalinger. For å undersøke dette er vi avhengig av å finne ut av hvilke utfordringer informantene har i forbindelse med IKT-sikkerhetsarbeid.

Er sikkerhetsarbeidet godt forankret i ledelsen?

Den første utfordringen vi ville utrede var forankring i ledelsen. Mange av informantene vi intervjuet var selv en del av ledelsen i sine bedrifter, så vi var nødt til å presisere at vi var ute etter toppledelsen eller den delen av ledelsen som er ansvarlig for å tildele ressurser til sikkerhetsarbeid.

I *Tabell* 4.6 har vi tydeliggjort hvilke informanter som er medlem av toppledelsen, og hvorvidt de syns sikkerhetsarbeidet er godt forankret i ledelsen.

Informant	Medlem av toppledelsen?	Er sikkerhetsarbeidet godt forankret i ledelsen?
CCO	Ja	Ja
CTO	Ja	Ja
CISO	Ja	Ja
Arkitekt 2	Ja	Ja
Arkitekt 1	Ja	Nei
Partner	Ja	Nei
Sivilarkitekt	Nei	Ja
IT-manager	Nei	Ja
Daglig leder	Nei	Ja
Landskapsarkitekt 1	Nei	Ja
Landskapsarkitekt 2	Nei	Ja

Tabell 4.6: Oversikt over hvilke informanter som er medlem av toppledelsen, sammenstilt med deres mening om hvorvidt sikkerhetsarbeidet er godt forankret i ledelsen

9 av 11 informanter opplever at sikkerhetsarbeidet er godt forankret i ledelsen. 2 informanter, hvorav begge er medlem av toppledelsen, opplever at det ikke er godt forankret i ledelsen og gir følgende begrunnelse for vurderingen:

Arkitekt 1 – «Om jeg generelt kan si at det er det, nei det kan jeg ikke. Vi har fokus på det, men det er ikke noe sånt sentralt punkt i vår daglige drift»

Partner – «Når vi ikke jobber med det, så er det ikke det»

2 av informantene som oppgir at sikkerhetsarbeidet er godt forankret i ledelsen begrunner det med at «ingen i ledelsen er motstandere av IKT-sikkerhet».

Får sikkerhetsarbeidet tilstrekkelig med midler?

9 av de 11 informantene opplever at sikkerhetsarbeidet får tilstrekkelig med midler. De som opplever at det ikke gjør det gir følgende forklaring:

Partner - Informanten sier at det ikke avsettes noen midler til det løpende sikkerhetsarbeidet i bedriften. Sikkerhet får tildelt midler kun ved behov, altså det settes av midler så snart det blir akutt.

CISO - På spørsmålet svarer informanten at det må være en balansegang når det kommer til tildeling av midler til sikkerhetsarbeidet. På grunn av at bedriften er i oppstartsfasen, så er de avhengige av å tjene penger og sikkerhetsarbeid tar tid som kan brukes på verdiskapende aktiviteter. Informanten avslutter med å si at de er klare over at det ikke kan fortsette på denne måten om de skal kunne vokse ytterligere.

Har ansatte med ansvar for IKT-sikkerhet tilstrekkelig med kapasitet og kompetanse for å utføre arbeidet slik de ser nødvendig?

Den andre utfordringen vi ville utrede var om ansatte med ansvar for IKT-sikkerhet innehar tilstrekkelig kompetanse og kapasitet. Her vil vi utelukke de som tjenesteutsetter sikkerhetskopiering, da disse informantene opplyser om at manglende kompetanse og kapasitet er årsaken til at de velger å benytte en ekstern IKT-driftsleverandør.

I og med at alle informantene vi prater med har et overordnet ansvar for IKT-sikkerhet i sin bedrift, blir de i dette spørsmålet nødt til å gjøre en selvevaluering av egen kapasitet og kompetanse på IKT-sikkerhet. Under beskrives hva vi legger i kompetanse og kapasitet.

Kompetanse: Omhandler at den som har ansvar for IKT-sikkerhet i en bedrift vet hvordan man skal beskytte bedriften sine systemer og data. Om man tjenesteutsetter IT-drift så omhandler kompetanse at man vet hva man trenger fra tredjepart og at man vet hvordan man kontrollerer at de gjennomfører det som er avtalt.

Kapasitet: Handler om at den ansvarlige for IKT-sikkerhet kan avse nok av sin arbeidstid, for å sørge for tilstrekkelig IKT-sikkerhet. Om man tjenesteutsetter, så omhandler kapasitet at man har tid til å følge opp tredjepart, for å sørge for at de leverer det som er avtalt.

Informant	Kompetanse	Kapasitet
IT-sjef	Ja	Ja
CCO	Nei	Ja
CTO	Nei	Ja
Landskapsarkitekt 2	Nei	Ja
CISO	Ja	Nei
Partner	Ja	Nei
Arkitekt 2	Nei	Nei

Tabell 4.7: Oversikt over hvorvidt informantene som ikke tjenesteutsetter sikkerhetskopiering mener å ha tilstrekkelig kompetanse og kapasitet til sikkerhetsarbeid

CCO - Informanten opplever at de som har ansvar for IKT-sikkerhet i bedriften har tilstrekkelig kapasitet til å utføre arbeidet, men at det skorter litt på kompetansen som kreves.

Landskapsarkitekt 2 - Informanten mener de har kapasitet, men ikke kompetanse. De tjenesteutsetter deler av sin IT-drift og forteller at de er veldig avhengig av gode råd fra leverandør for å vite hva de har behov for.

Øvrige utfordringer

I tillegg til de kjente utfordringene for IKT-sikkerhet, som vi hadde spørsmål om i intervjuet, kom det også frem noen andre utfordringer som enkelte av informantene hadde.

CTO - Informanten forteller at den største utfordringen de har, er at de ikke har hatt bestillerkompetanse internt.

CISO - Informanten mener at alle som jobber med teknologi bør ha et visst nivå av IT-sikkerhet i utdannelsen. Informanten opplever at utviklere i egen bedrift ikke har god nok kompetanse på IT-sikkerhet, grunnet at man ikke lærer nok om det i utdanningen.

CCO - Informanten mener at kompetansen de innehar på IKT-sikkerhet for øyeblikket er tilstrekkelig, men at hvis de vil sette det i et større system er de nødt til å ha egne folk som jobber bare med dette. Informanten mener det er vanskelig å få tak i folk, og at utfordringen er at det ikke utdannes nok folk som jobber med IKT-sikkerhet.

Landskapsarkitekt 2 – Informanten opplever at den største utfordringen bedriften møter på, er at de ansatte ikke forstår viktigheten av god IKT-sikkerhet. Informanten sier følgende: «Bare det å implementere MFA, har møtt såpass motstand at vi har utsatt det».

4.6 Resultater fra oppfølgingsundersøkelsen

Hensikten med oppfølgingsundersøkelsen var å finne ut om intervjuene hadde hatt noen påvirkning på informantene. 9 av 11 informanter besvarte spørreundersøkelsen. Under presenteres relevante svar.

HAR DERE TENKT TIL Å TA I BRUK ET RAMMEVERK FOR IKT-SIKKERHET ETTER VI HADDE INTERVJU MED DEG?

6 informanter svarer at de planlegger å ta i bruk et rammeverk for IKT-sikkerhet i etterkant av intervjuet vi hadde med dem. Samtlige svarer at de tenker å bruke NSMs-grunnprinsipper som hjelpemiddel når de skal utvikle dette rammeverket.

DERSOM DERE TJENESTEUTSETTER IT-DRIFT, HAR DERE GJENNOMFØRT LEVERANDØRKONTROLL I ETTERKANT?

1 informant svarer at de har gjennomført leverandørkontroll, og ytterligere 4 informanter svarer at de planlegger å gjøre det.

HAR DERE GJENNOMGÅTT KONTRAKT MED IT-LEVERANDØREN DERES ETTER VI HADDE INTERVJU MED DEG?

1 informant svarer at de har gjennomgått kontrakt med IT-leverandør etter vi hadde intervju.

KAN DU UTDYPE DERSOM DERE HAR GJORT NOEN ENDRINGER I DERES SIKKERHETSKOPIERINGSPRAKSIS I ETTERKANT AV INTERVJUET?

1 informant oppgir at de gjort endringer i sikkerhetskopieringspraksisen til bedriften ved at de har begynt å teste sikkerhetskopiene. Videre oppgir 1 informant følgende svar:

> *«Foreløpig har vi kun planlagt litt internt ved å først samle inn dokumentasjon vi har rundt våre avtaler og rutiner. Så skal vi skrive ned spørsmål om ting vi er usikre på hvordan håndteres rundt IKT-sikkerheten vår som vi skal stille vår eksterne IT-konsulent. Vi ønsker blant annet å vite hvordan man tester sikkerhetskopier og hvem som gjennomfører det.»*

HAR DERE SNAKKET MER OM IKT-SIKKERHET I ETTERKANT AV INTERVJUET?

Av 9 informanter er det 6 som oppgir at de har snakket mer om IKT-sikkerhet i etterkant av intervjuet. 3 av informantene oppgir at de har diskutert det internt, mens 1 har i tillegg diskutert det med IKT-driftsleverandør. 1 av informantene skriver følgende:

> *«Vi har påbegynt en kartlegging av hva vi har, og hva vi burde forbedre. Når vi får en tydelig avklaring rundt hvilke nødvendige rutiner som allerede er dekket vil vi påse at vi får på plass det som mangler. Vi*

vil også utarbeide et informasjonsskriv til intern bruk som beskriver hva vi må gjøre i ulike situasjoner (dersom de oppstår).»

FØRTE INTERVJUET TIL NOE ANNET, SOM IKKE NEVNT I SPØRSMÅLENE OVER?

Her svarte 3 informanter at intervjuet førte til ytterligere bevisstgjøring av IKT-sikkerhet innad i bedriften.

5 Diskusjon

5.1 Introduksjon

I dette kapittelet skal vi diskutere resultatene sett opp mot forskningsspørsmålene. Vi vil trekke frem interessante funn og røde tråder. Avslutningsvis diskuterer vi forskningens troverdighet.

5.2 Informantenes åpenhet og innsikt i IKT-sikkerhet

Vi opplevde at samtlige informanter var godt egnet til å besvare spørsmål knyttet til IKT-sikkerhet i sine bedrifter. Selv om IKT-sikkerhet ikke var spesifisert i stillingsbeskrivelsen til alle informantene, opplevde vi at snakket med den personen i bedriften som var best egnet til å besvare våre spørsmål. Vi var bekymret for at informantene ville pynte på sannheten for å gjøre et bedre inntrykk, men vi opplevde at de var svært ærlige og åpne om feil og mangler. Åpenheten til informantene la til rette for en god dialog.

5.3 Forskningsspørsmål 1

I hvilken grad samsvarer bedrifters rutiner og prosesser for sikkerhetskopiering med NSMs anbefalinger?

For å besvare forskningsspørsmål 1 tar vi utgangspunkt i resultatene fra kategori 2. I denne kategorien besvarer informantene hvorvidt rutinene og prosessene deres for sikkerhetskopiering samsvarer med NSM sine anbefalinger. Antall poeng informantene har fått er basert på metrikkene fra Tabell 3.7 og utregning for den enkelte er vedlagt i *Vedlegg 4: Informantenes etterlevelse av prinsipp 2.9*. Resultatene i tabellen viser i hvor stor grad sikkerhetskopieringspraksiser hos hver enkelt informant sin bedrift, samsvarer med NSM sine anbefalinger.

Informant	**Poeng**	**Grad av samsvar med NSMs anbefalinger på sikkerhetskopiering**
CISO	24/40	Middels
Landskapsarkitekt 1	23/40	Middels
Arkitekt 1	22/40	Middels
IT-sjef	22/40	Middels
CCO	14/40	Middels
Daglig leder	10/40	Lav
CTO	9/40	Lav
Sivilarkitekt	3/40	Lav
Arkitekt 2	2/40	Lav
Landskapsarkitekt 2	2/40	Lav
Partner	0/40	Lav

Tabell 5.1: Oversikt over i hvilken grad informantenes sikkerhetskopieringspraksiser samsvarer med NSMs anbefalinger

Det er betydelige variasjoner i hvor høy grad bedriftenes praksis for sikkerhetskopiering samsvarer med NSM sine anbefalinger. De mest sentrale punktene for våre informanter er følgende:

- Det viktigste tiltaket NSM trekker frem i forbindelse med sikkerhetskopiering er at virksomheter må ha en plan for det. De 5 informantene som oppnår lavest etterlevelse mangler alle en slik plan.
- Ingen av informantene oppgir at de tester sikkerhetskopiene sine regelmessig.
- Det er kun 2 informanter som tilfredsstiller alle fire punktene, som NSM mener er et minimum for å beskytte sikkerhetskopiene.
- Det kommer også frem at de som benytter seg av en IKT-driftsleverandør, i liten grad har oversikt over hvordan sikkerhetskopiene beskyttes.

5.4 Forskningsspørsmål 2

«Hvilke forhold påvirker etterlevelsen av NSMs anbefalinger?»

For å besvare forskningsspørsmål 2 ser vi på helheten av det som kommer frem fra dybdeintervjuene. Særlig er kategori 3 relevant, men det vil også bli trukket frem resultater fra de andre kategoriene. I undersøkelsen vår fant vi følgende forhold som kan påvirke etterlevelsen av NSMs anbefalinger:

1) Bruk av rammeverk for IKT-sikkerhet
2) Kompetanse og kapasitet
3) Leverandørkontroll ved tjenesteutsetting
4) Bestillerkompetanse
5) Opplevd datatap med økonomiske konsekvenser

Vi vil nå diskutere disse og avslutningsvis se på hvilken måte bevissthet påvirker hvert enkelt av disse forholdene.

5.4.1 Forhold 1: Bruk av rammeverk for IKT-sikkerhet

I vår undersøkelse opplyste 4 av 11 informanter at bedriften følger et rammeverk for IKT-sikkerhet, vist i *Tabell* 5.2.

Informant	**Rammeverk**	**Grad av samsvar med NSMs anbefalinger på sikkerhetskopiering**
CISO	NSMs grunnprinsipper for IKT-sikkerhet	Middels
IT-sjef	NSMs grunnprinsipper for IKT-sikkerhet og ISO27001	Middels
CCO	Egenutviklet rammeverk, subsett av etablerte rammeverk	Middels
Sivilarkitekt	Egenutviklet rammeverk	Lav

Tabell 5.2: Tabell som viser hvilke rammeverk informantene følger, sammenstilt med resultat fra tabell 5.1

3 av informantene som følger et rammeverk for IKT-sikkerhet er i toppsjiktet av bedriftene vi har intervjuet, når det kommer til hvor høy grad deres praksis for sikkerhetskopiering samsvarer med NSMs anbefalinger. Den siste bedriften er ikke i

toppsjiktet, men i motsetning til de tre andre bedriftene, er ikke dette rammeverket basert på et etablert rammeverk. Resultatene fra undersøkelsen peker mot at det å følge et rammeverk for IKT-sikkerhet er et forhold som påvirker etterlevelsen til NSMs anbefalinger, med den forutsetning at rammeverket innehar nødvendige sikringstiltak. Dette kan oppnås ved å følge etablerte og anbefalte rammeverk, slik som de i *Tabell* 5.3, eller å etablere sitt eget rammeverk basert på disse.

I likhet med andre etablerte rammeverk for IKT-sikkerhet er også NSMs grunnprinsipper tett knyttet opp mot ISO/IEC 27002 og beste praksiser innen informasjonssikkerhet. Dermed vil det være en rekke likheter mellom de ulike IKT-rammeverkene. Forskjellen går på valg av tiltak, hvor noen rammeverk er mer omfattende enn andre, i tillegg til at noen er mer utdypende. For å belyse dette kan vi se på sammenhengen mellom et utvalg rammeverk og hvorvidt de innehar tiltak for testing av sikkerhetskopier. Rammeverkene som trekkes frem i *Tabell* 5.3*,* er et utvalg etablerte rammeverk man kan benytte.

Rammeverk	**Tiltak nr.**	**Tiltak**
NSMs grunnprinsipper	2.9.3	Test sikkerhetskopier regelmessig ved å utføre gjenopprettingstest for å verifisere at sikkerhetskopien fungerer [19, s. 35].
ISO 27002	12.3.1	Sikkerhetskopier av informasjon, programvare og systemavbildninger skal tas og testes regelmessig i samsvar med en avtalt policy for sikkerhetskopiering [22, s. 45].
CIS CSC v8	11.5	*Test backup recovery quarterly, or more frequently, for a sampling of in-scope enterprise assets* [24, s. 37].
NIST Cybersecurity Framework	PR.IP-4	*Backups of information are conducted, maintained, and tested* [37, s. 34].

Tabell 5.3: Tabell som sammenligner tiltak fra forskjellige rammeverk for IKT-sikkerhet

Med denne sammenstillingen viser vi likhetene mellom ulike rammeverk for IKT-sikkerhet og at å følge et etablert rammeverk for IKT-sikkerhet er et av forholdene som påvirker etterlevelsen av NSMs anbefalinger.

5.4.2 Forhold 2: Kompetanse og kapasitet

Det krever kompetanse og kapasitet for å ha høy etterlevelse av NSMs anbefalinger. For å belyse dette kan vi se på hvordan kompetanse og kapasitet kreves for å etterleve prinsipp 2.9. For det første kreves det en grad av kompetanse for å forstå konsekvensen av datatap og hvor viktig det er å ha en god sikkerhetskopieringspraksis av virksomhetskritisk data. Videre kreves det kompetanse og kapasitet for å implementere en sikkerhetskopieringspraksis som leder til høy etterlevelse av prinsipp 2.9. I den forbindelse kreves det teknisk kompetanse for å vite hvordan man skal utføre sikkerhetskopieringen og beskytte sikkerhetskopiene. Dessuten kreves det at de som innehar kompetanse til dette har tilstrekkelig kapasitet til å utføre arbeidet. Beslutningstakere som skal tildele midler må dermed forstå at sikkerhetsarbeid er tidkrevende, og sørge for at de som utfører arbeidet har tilstrekkelig kompetanse og kapasitet.

Et utgangspunkt for å beskytte seg mot datatap, er at bedriften har oversikt over hvilke verdier de må beskytte. Alle informantene trekker frem hvilke digitale verdier de anser

som virksomhetskritiske. Videre gir informantene reflekterte svar knyttet til hva det vil koste dem om de digitale verdiene blir utilgjengelig midlertidig eller permanent. Vi opplever med det at informantene forstår konsekvensene av datatap.

Kun 1 informant mener å inneha tilstrekkelig kompetanse og kapasitet til å utføre IKT-sikkerhetsarbeid slik de ser det nødvendig. Dersom en mangler kompetanse og kapasitet til sikkerhetsarbeid er trolig tjenesteutsetting riktig avgjørelse. 4 av informantene oppgir at de tjenesteutsetter sikkerhetskopiering og at årsaken til det er at de mangler tilstrekkelig kompetanse og kapasitet til å utføre arbeidet selv. Resterende 6 informanter oppgir at de mangler enten kompetanse eller kapasitet, men likevel utfører sikkerhetskopiering selv. Kanskje skulle disse informantene også vurdert å tjenesteutsette sikkerhetskopiering, på det grunnlag at en må inneha både kompetanse og kapasitet for å utføre det på en god måte.

Tre informanter trekker frem manglende kompetanse hos øvrige ansatte som den største utfordringen deres når det kommer til IKT-sikkerhetsarbeid. En informant opplyser om at implementering av MFA møtte så stor motstand hos ansatte at det ble utsatt. I dette tilfellet så ble et helt sentralt sikkerhetstiltak hindret på grunn av at øvrige ansatte manglet kompetanse til å forstå viktigheten. En annen informant trekker frem at manglende kompetanse på IKT-sikkerhet hos deres utviklere er en stor utfordring for dem, mens den siste informanten ser for seg at bedriften vil slite med videre utvikling dersom de ikke får ansatt flere personer med IKT-sikkerhetsekspertise. Disse refleksjonene peker mot at en grad av kompetanse på IKT-sikkerhet er viktig for alle ansatte, ikke bare de som har ansvar for IKT-sikkerhet i bedriften.

Som vist i *Tabell* 5.1 har ingen av informantene høy etterlevelse av prinsipp 2.9. Basert på vår undersøkelse er manglende kompetanse og kapasitet en av årsakene til det. Dette tyder på at tilstrekkelig kompetanse og kapasitet er et av forholdene som påvirker etterlevelsen av NSMs anbefalinger. Vi vil i avsnitt 5.4.3 diskutere mulige årsaker til at de som tjenesteutsetter ikke har høy etterlevelse.

5.4.3 Forhold 3: Leverandørkontroll ved tjenesteutsetting

Som vist i avsnitt *5.4.2* er bedrifter som organiserer IT-drift internt avhengig av å ha tilstrekkelig kompetanse og kapasitet for å etterleve NSM sine anbefalinger til høy grad. Det er et modent valg av de informantene som opplever at de mangler det, å tjenesteutsette arbeidet, men da kreves det i gjengjeld god leverandørkontroll.

Gjennom intervjuene, kom det frem følgende for de 6 informantene som helt eller delvis har tjenesteutsatt sin IT-drift:

- Ingen hadde gjennomført noen form for kontroll av IKT-driftsleverandør.
- Ingen av de som tjenesteutsatte sikkerhetskopiering hadde gjennomført en gjenopprettingstest av sikkerhetskopien, annet enn ved behov.
- Ingen av informantene som tjenesteutsetter sin IT-drift hadde full kontroll på IKT-driftsleverandør sin praksis og hva som inngikk i avtalen.

Selv om man overlater IT-driften til en tredjepart, så er det fremdeles viktig å ha oversikt over avtalen, og regelmessig kontrollere at tredjepart overholder den. Dette er fordi at risikoen for IKT-sikkerhetshendelser fortsatt eies av bedriften som tjenesteutsetter. Et godt sitat fra en informant er «Du kan ikke outsource risiko, den eier

du selv». NSM understreker viktigheten av dette ved å vurdere tiltak *2.1.9 Ta ansvar for virksomhetens sikkerhet også ved tjenesteutsetting* [19, s. 19-20] som 1 av de 15 tiltakene innenfor prioriteringsgruppe 1. Tiltaket presiserer blant annet at det er viktig å ha oversikt og kontroll på hele livsløpet til tjenesten som utsettes og at det bør utarbeides et kravdokument for alle faser av tjenesteutsetting hvor krav kan verifiseres.

NSMs grunnprinsipper kan benyttes av bedrifter som tjenesteutsetter, ved at de kan stille krav til sin leverandør om å følge dem. Dette vil hjelpe bedriftene med å etterleve prinsippene, selv om de ikke har den tekniske kompetansen til å gjøre dette selv. I tillegg vil da leverandørkontroll kunne gjennomføres på en systematisk måte, ved at bedriftene kan kontrollere sin IKT-driftsleverandør ved hjelp av NSMs grunnprinsipper. For de som tjenesteutsetter vil derfor leverandørkontroll være et av forholdene som påvirker etterlevelsen av NSMs anbefalinger.

5.4.4 Forhold 4: Bestillerkompetanse

En informant opplyser om at bestillerkompetanse er den største utfordringen deres når det kommer til IKT-sikkerhetsarbeid. Informanten sier at ledelsen forstår viktigheten av god IKT-sikkerhet, men at de selv ikke innehar kompetansen til å velge riktige tjenester hos en IKT-driftsleverandør. Det kan være at det er flere av informantene som mangler god bestillerkompetanse, men dette ble ikke undersøkt hos samtlige av de vi intervjuet. Bakgrunnen for det utdypes i avsnitt 5.5 – *Forskningens troverdighet*. NSM anser bestillerkompetanse som en helt sentral faktor ved vellykket tjenesteutsetting. Det presiseres blant annet i tiltak 2.1.9 [19, s. 19-20], som nevnt tidligere er vurdert som 1 av de 15 viktigste tiltakene fra NSMs grunnprinsipper. Her skriver NSM at virksomheter må ivareta behovet for bestillerkompetanse gjennom hele livsløpet til tjenesteutsettingen.

Da vi diskuterte kompetanse og kapasitet trakk vi frem at flere informanter begrunner behovet for tjenesteutsetting på bakgrunn av manglende kompetanse og kapasitet til IKT-sikkerhetsarbeid. I teorikapittelet forklarte vi hvordan god bestillerkompetanse blant annet krever grunnleggende IKT-kompetanse. I ettertid ble vi oppmerksomme på at denne situasjonen kan være krevende dersom det er manglende kompetanse som er hovedårsaken til tjenesteutsetning av IT-drift. I den anledning kan det være vanskelig å opprettholde god bestillerkompetanse.

NSMs grunnprinsipper kan med fordel benyttes av bedrifter som hjelpemiddel i prosessen når de skal kjøpe tjenester fra IKT-driftsleverandører. NSM har for hvert prinsipp i grunnprinsippene et avsnitt som heter «Hvorfor er dette viktig». Dette punktet kan bidra til å belyse hvilke utfordringer prinsippet søker å løse, og hvilke tiltak som anbefales å gjennomføres i den forbindelse. Vi mener at dersom bedrifter benytter seg av dette hjelpemidlet i prosessen, vil de ha et godt utgangspunkt for en vellykket tjenesteutsetting av IT-drift, og bestillerkompetanse vil derfor være et forhold som påvirker etterlevelsen av NSMs anbefalinger.

5.4.5 Forhold 5: Opplevd datatap med økonomiske konsekvenser

«Det kommer til å bli verre, før det kan bli bedre»

Uttrykket over brukes i en rekke sammenhenger, også relatert til IKT-sikkerhet. For folk med lite IKT-kunnskap kan IKT-sikkerhet oppleves abstrakt, men når IKT-

sikkerhetshendelser oppstår blir plutselig konsekvensene reelle og håndfaste. Det er derfor interessant om bedriftene som har opplevd datatap, har skjerpet sine rutiner eller om det har ført til økt bevissthet rundt IKT-sikkerhet.

4 av informantene har opplevd datatap som medførte økonomiske konsekvenser. I Tabell 5.4 vises omfanget av datatapet.

Informant	Årsak til datatap	Konsekvens av datatap
Arkitekt 1	Løsepengevirus	Midlertidig utilgjengelig data medførte driftsstopp for hele bedriften i en halv arbeidsdag.
Arkitekt 2	Dårlige rutiner ved sikkerhetskopiering	Fører til tilfeller med permanent datatap. Informanten har ikke beregnet kostnadene knyttet til dette.
Landskapsarkitekt 2	En filserver krasjet	Flere dagers driftsstopp for hele bedriften. Ikke beregnet nøyaktig kostnad.
Partner	Usikker på årsaken	Opplever tilfeller med tap av data, men er ikke sikker på konsekvensen ved det.

Tabell 5.4: Årsak og konsekvens for informantene som har opplevd datatap

Ingen av informantene som har opplevd datatap har beregnet den økonomiske kostnaden det medførte og ingen har innført risikoreduserende tiltak i etterkant. For vår del kan vi verken bekrefte eller avkrefte om opplevd datatap er et forhold som påvirker etterlevelsen av NSMs anbefalinger i seg selv. Det nærmeste vi kommer er Arkitekt 1, som presiserte at hendelsen med løsepengevirus ikke førte til noen konkrete tiltak, men at bedriften i større grad satset på bevisstgjøring av IKT-sikkerhetsrutiner blant ansatte. Det kan være at det faktisk må bli verre, før det kan bli bedre, altså at hendelsene informantene opplever må være av en høyere alvorlighetsgrad, før de ser behovet for å innføre risikoreduserende tiltak.

5.4.6 Bevissthet relatert til forholdene

Fram til nå har vi diskutert hvorvidt følgende forhold påvirker etterlevelsen til NSMs anbefalinger:

- Bruk av rammeverk for IKT-sikkerhet
- Kompetanse og kapasitet
- Leverandørkontroll
- Bestillerkompetanse
- Opplevd datatap med økonomiske konsekvenser

En felles faktor mellom disse forholdene er at de i stor grad handler om bevissthet. Vi vil nå diskutere hvordan bevissthet påvirker hvert enkelt av disse forholdene.

Bruk av rammeverk for IKT-sikkerhet

Tidligere viste vi at det å følge et rammeverk for IKT-sikkerhet var et forhold som påvirket etterlevelsen til NSMs anbefalinger. I den forbindelse kan det være interessant å se på hvilke faktorer som påvirker om bedrifter i utgangspunktet velger å følge et

rammeverk for IKT-sikkerhet. Alle informantene opplyste om at de både har midlene til det og støtte fra ledelsen til å prioritere IKT-sikkerhet, men bare fire av de oppgir at de følger et rammeverk for IKT-sikkerhet. Slik vi ser det er det to ulike årsaker til at de resterende 7 informantene ikke tar i bruk rammeverk for IKT-sikkerhet:

1. De er bevisste på fordelene ved å ta i bruk et rammeverk for IKT-sikkerhet, men velger å ikke ta det i bruk
2. De er ikke bevisste på fordelene ved å ta i bruk et rammeverk for IKT-sikkerhet

6 av 11 informanter svarte at de i forkant av intervjuet ikke hadde hørt om NSMs grunnprinsipper for IKT-sikkerhet. Som en effekt av dybdeintervjuet fikk informantene økt bevissthet om NSMs grunnprinsipper for IKT-sikkerhet. I oppfølgingsundersøkelsen svarte 6 informanter, som tidligere ikke fulgte et rammeverk, at de nå har tenkt å implementere det i bedriften. Videre svarte samtlige av disse informantene at de skal bruke NSMs grunnprinsipper for IKT-sikkerhet som et hjelpemiddel. Derfor mener vi at det er årsak nummer 2, altså at de er ikke bevisste på fordelene ved å ta i bruk et rammeverk for IKT-sikkerhet, som gjør at bedriftene ikke følger et rammeverk for IKT-sikkerhet. Våre funn indikerer dermed at økt bevissthet på fordelene av å følge et rammeverk for IKT-sikkerhet, førte til at de valgte å implementere det.

Kompetanse og kapasitet

Det er ledelsen som sitter med overordnet ansvar for IKT-sikkerheten i bedriften sin. Det er også som regel ledelsen som er endelige beslutningstakere når det kommer til håndtering av risikoer og fordeling av midler til IKT-sikkerhetsarbeid. I den anledning er ledelsen nødt til å være bevisst på at IKT-sikkerhetsarbeid er en kontinuerlig prosess, som krever at ansvarlige har tilstrekkelig kompetanse og kapasitet til å utføre arbeidet.

Leverandørkontroll

For de informantene som tjenesteutsetter IT-drift er det to funn som er sentrale:

1. Ingen av informantene hadde full kontroll på hva som inngår i avtalen med IKT-driftsleverandør
2. Ingen av informantene hadde gjennomført leverandørkontroll

Funnene over tyder på at informantene enten var lite bevisste på, eller ikke tok ansvar for egen risiko. Gjennom intervjuene fikk informantene spørsmål relatert til praksisen til IKT-driftsleverandør og hvorvidt de kontrollerte om avtalen ble overholdt. Det kan tenkes at informantene opplevde det som ubehagelig at de ikke kunne svare godt på disse spørsmålene og at det førte til en bevisstgjøring på viktigheten av leverandørkontroll. Resultatene fra oppfølgingsundersøkelsen indikerer at dette var tilfellet. I oppfølgingsundersøkelsen svarte 1 informant at de har gjennomført leverandørkontroll, mens 4 svarer at de planlegger å gjennomføre det. I tillegg er det en informant som oppgir å ha revidert kontrakten med IKT-driftsleverandør som et resultat av intervjuet.

Bestillerkompetanse

Det vi oppdaget gjennom intervjuene var at bevissthet på hjelpemidler kan være til hjelp for å øke bestillerkompetanse. Bedrifter som tjenesteutsetter IT-drift bør være:

1. Bevisste på at god bestillerkompetanse er en forutsetning for vellykket tjenesteutsetting av IT-drift

2. Bevisste på hvilke hjelpemidler man kan ta i bruk for å øke bestillerkompetansen.

De som har opplevd datatap

Vi ønsket å undersøke om de informantene som hadde opplevd datatap med økonomiske konsekvenser var mer bevisste på konsekvensene, og om dette medførte økt robusthet mot datatap. Bevissthet på konsekvenser er trolig et forhold, men fra vår undersøkelse var det vanskelig å trekke ut noe konkret, da informantene ikke fikk alvorlige økonomiske konsekvenser som følge av datatap de hadde opplevd.

5.5 Forskningens troverdighet

En sentral del av forskningsprosessen er å forsikre at man kan trekke gyldige slutninger fra resultatene. Det er dermed viktig å vurdere kvaliteten og troverdigheten av dataen som er samlet inn i løpet av oppgaven.

For det første er det en skjevfordeling av informantenes bransjetilhørighet, da seks av informantene er ansatt i arkitektbransjen. Bransjetilhørighet påvirker i liten grad resultatene, av den årsak at sikkerhetskopieringspraksiser er noe alle som forvalter digitale verdier må ta stilling til på tilnærmet likt grunnlag.

Videre har vi ikke kontrollert at det som informantene fortalte gjennom intervjuene stemmer med realiteten. Siden de vi intervjuet var ansvarlige for IKT-sikkerhet i sin bedrift, kunne det tenkes at de ville pynte på situasjonen og unnlate å oppgi relevant informasjon om deres egne mangler. Dette var kanskje tilfellet for noen, da vi opplevde at enkelte svarte positivt på noen av spørsmålene, men ved videre diskusjon kom det fram at det egentlig ikke var helt slik det ble framstilt i utgangspunktet. Ved å bruke dybdeintervju som metode, mener vi at vi klarte å avdekke hvordan situasjonen faktisk var for de fleste. Totalt sett opplevde vi at de fleste var oppriktige og vi vurderer det som sannsynlig at vi gjennom samtale klarte å rette opp i misforståelser og at resultatene vi fikk derfor stemmer med realiteten.

I forbindelse med forskningsspørsmål 1 vurderte vi informantenes grad av samsvar med NSMs anbefalinger på sikkerhetskopiering vist i *Tabell* 5.1. I de situasjonene hvor informantene manglet oversikt over hva IKT-driftsleverandøren gjorde eller hva som var avtalt dem imellom, fikk de ikke uttelling på samsvar med NSMs anbefalinger. Som et resultat av dette, kan det være at vi har underestimert bedriftenes reelle etterlevelse. Til tross for dette mener vi at målingene har nytteverdi, grunnet at vi valgte å legge vekt på at informantene tok ansvar for IKT-sikkerhet i egen bedrift.

I spørsmål nummer 3 fra intervjuguiden stiller vi informantene følgende spørsmål: «På en skala fra 1 til 10, hvor stort fokus mener du at din bedrift har på IKT-sikkerhet?». Vi tenkte at dette kunne si noe om bedriftenes modenhet og bevissthet på IKT- sikkerhet, og at vi kunne bruke resultatene til å sammenligne deres mening, med det vi fant i analysen. Vurderingen informantene gjør på dette spørsmålet er kun basert på deres egen kunnskap og erfaringer. Det innebærer at det en informant vurderer til å tilsvare verdien 10, kan tilsvare 5 for en annen informant. Det samme gjelder for vår egen vurdering av tallverdiene. Det gikk først opp for oss i etterkant av intervjuene at en sammenligning av informantene sine svar ville være lite holdbar. Begrunnelsene informantene ga for å forsvare egen vurdering var derimot interessante, og vi valgte med det å beholde avsnittet i resultatkapittelet.

Vi gjennomførte 11 intervjuer og underveis i prosessen dukket det opp ulike utfordringer informantene hadde med IKT-sikkerhet, som vi ikke hadde tenkt på da vi utarbeidet intervjuguiden. Et eksempel på dette er utfordringen med bestillerkompetanse. Vi ble først gjort oppmerksomme på denne utfordringen i intervju nummer 7. Vi syntes dette var interessant og valgte å spørre resterende informanter om denne utfordringen, dette medførte at intervjuene gradvis ble endret etter hvert som vi oppdaget nye områder vi ville utforske. Problemet med dette var at ikke alle informantene ble stilt de samme spørsmålene og at noen av svarene vi fikk manglet sammenligningsgrunnlag. Siden vi var ute etter å avdekke utfordringer vi ikke visste om og som kunne bidra til å finne løsninger for å øke etterlevelsen av NSMs anbefalinger, var vi ikke avhengig av å sammenligne alle svarene vi fikk. Vi anser derfor ikke dette som et stort problem, men det kunne allikevel vært interessant å få alle informantenes synspunkter rundt utfordringene som ble oppdaget underveis.

6 Konklusjon

6.1 Forskningsspørsmål 1

I hvilken grad samsvarer bedrifters rutiner og prosesser for sikkerhetskopiering med NSMs anbefalinger?

Fra dybdeintervjuene våre, kommer det frem at bedrifters rutiner og prosesser for sikkerhetskopiering samsvarer i lav til middels grad med NSMs anbefalinger. 6 av bedriftene hadde lav grad av samsvar, mens 5 hadde middels. Ved å bruke sikkerhetskopieringspraksisene som en indikator på bedriftenes modenhet og generelle IKT-sikkerhetstilstand antyder denne målingen at det er behov for å øke etterlevelsen av NSMs anbefalinger hos SMB.

6.2 Forskningsspørsmål 2

Hvilke forhold påvirker etterlevelsen av NSMs anbefalinger?

Basert på vår undersøkelse har følgende forhold påvirkning på etterlevelsen av NSMs grunnprinsipper for IKT-sikkerhet:

Bruk av rammeverk for IKT-sikkerhet: Det fører til økt etterlevelse av NSM anbefalinger, dersom en bedrift følger et etablert rammeverk for IKT-sikkerhet eller baserer seg på et etablert rammeverk for å lage sitt eget.

Kompetanse og kapasitet: Ansatte med ansvar for IKT-sikkerhetsarbeid må ha både tilstrekkelig kompetanse og kapasitet for å kunne etterleve NSMs anbefalinger. Det er også viktig at øvrige ansatte innehar en grad av kompetanse.

Leverandørkontroll: Ved tjenesteutsetting er man avhengig av god leverandørkontroll om man skal etterleve NSMs anbefalinger. Bedrifter kan da stille krav til leverandør om å følge NSMs anbefalinger og kontrollere at avtalen overholdes.

Bestillerkompetanse: Dersom NSMs grunnprinsipper for IKT-sikkerhet benyttes som et hjelpemiddel i prosessen ved bestilling av tjenester fra en IKT-driftsleverandør vil dette være et forhold som påvirker etterlevelsen av NSMs anbefalinger.

Økt bevissthet viser seg å ha en positiv effekt på alle disse forholdene. Vi vil nå utdype hvordan vi oppnådde en bevissthetsøkning hos informantene våre, og på den måten bidro til å øke etterlevelsen av NSMs grunnprinsipper for IKT-sikkerhet.

6.3 Svar på problemstillingen

Hvordan kan man øke etterlevelsen av NSMs grunnprinsipper for IKT-sikkerhet?

Vi finner det særlig bemerkelsesverdig hvor stor effekt intervjuene hadde på informantene. Oppfølgingsundersøkelsen ble sendt ut omkring en måned i etterkant av intervjuene, og allerede da hadde mange av informantene påbegynt konkrete tiltak for å forbedre bedriftens IKT-sikkerhet. Det at informantene ble utfordret på deres IKT-sikkerhet og ble bevisstgjort nytteverdien av NSMs grunnprinsipper for IKT-sikkerhet som et hjelpemiddel, resulterte i en konkret økning i etterlevelsen. I oppfølgingsundersøkelsen kommer det frem at:

- 6 av 7 informanter som tidligere ikke fulgte et rammeverk for IKT-sikkerhet har nå besluttet å ta det i bruk. Samtlige oppgir at NSMs grunnprinsipper for IKT-sikkerhet vil bli benyttet som hjelpemiddel.
- 1 informant har gjennomført leverandørkontroll.
- 4 informanter planlegger å gjennomføre leverandørkontroll.
- 1 informant har gjennomgått kontrakten med IKT-driftsleverandør.

Med disse funnene ser vi at etterlevelsen kan økes, gjennom å bevisstgjøre bedrifter på nytteverdien av å benytte NSMs grunnprinsipper for IKT-sikkerhet som et hjelpemiddel i forbindelse med:

- etablering av et rammeverk for IKT-sikkerhet i egen bedrift
- bestilling av tjenester fra IKT-driftsleverandør
- gjennomføring av leverandørkontroll

6.4 Videre arbeid

I denne bacheloroppgaven har vi sett på hvordan SMB forholder seg til IKT-sikkerhet. Vi har kontrollert et utvalg av NSMs grunnprinsipper for IKT-sikkerhet, med fokus på sikkerhetskopiering. For å undersøke ytterligere kunne det vært interessant å:

Kontrollere et større utvalg av NSMs grunnprinsipper – Istedenfor å kun bruke sikkerhetskopiering som indikator på en bedrifts modenhet og generelle IKT-sikkerhetstilstand, vil man ved å kontrollere flere av prinsippene få et mer nøyaktig bilde.

Intervjue flere bedrifter for å få et større datagrunnlag – I undersøkelsene våre intervjuet vi 11 informanter, med en overvekt fra én bransje. Et større datagrunnlag vil legge til rette for et mer helhetlig bilde over etterlevelsen av NSM grunnprinsipper hos SMB. Det kan i tillegg muliggjøre at man avdekker øvrige forhold som påvirker etterlevelsen.

Gjennomføre oppfølgingsintervjuer – Framfor å følge opp informantene med spørreundersøkelser, kan det være fordelaktig å benytte intervjuer. I oppfølgingsintervjuene kan mange av de samme spørsmålene bli stilt. Da kan man sammenligne svar fra første og andre intervjurunde for å kontrollere om IKT-sikkerheten i bedriften og bevissthet rundt IKT-sikkerhet ble forbedret. Intervjuer legger i større grad til rette for at man kan undersøke økninger i etterlevelsen av NSMs grunnprinsipper hos bedriftene.

Referanser

[1] A. Tjora, *Kvalitative Forskningsmetoder i praksis*, 2. utg. Norge: Gyldendal Norsk Forlag AS, 2021.

[2] Store norske leksikon, «Informant.» SNL.no. Hentet fra: https://snl.no/informant (Lastet ned: 16.03.2023).

[3] Datatilsynet, «Iverksette styringssystem for informasjonssikkerhet.» Datatilsynet.no. Hentet fra: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/iverksette-styringssystem-for-informasjonssikkerhet/ (Lastet ned: 05.05.2023).

[4] *Forskrift om virksomheters arbeid med forebyggende sikkerhet (Virksomhetsforskriften),* 2019. [Online]. Hentet fra: https://lovdata.no/dokument/SF/forskrift/2018-12-20-2053

[5] European Union Agency for Cybersecurity, «Threat Landscape for Supply Chain Attacks.» 29.07.2021. [Online]. Hentet fra: https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks (Lastet ned 11.05.2023).

[6] Datsatilsynet, «Phishing - hvordan beskytte virksomheten.» Datatilsynet.no. Hentet fra: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/phishing---hvordan-beskytte-virksomheten/ (Lastet ned 05.05.2023).

[7] D. Sutton, *Information risk management A practitioners guide Second edition*, 2.utg. England: BCS Learning and Development Ltd, 2021.

[8] Sikt, «Sikt.» Sikt.no. Hentet fra https://sikt.no (Lastet ned 19.05.2023).

[9] B. M. Vikøren, R. Pihl. «Outsourcing.» SNL.no. Hentet fra: https://snl.no/outsourcing (Lastet ned 22.03.2023).

[10] NRK. «Hacket kommune får 16 millioner kroner i statsstøtte.» NRK.no. Hentet fra: https://www.nrk.no/innlandet/ostre-toten-kommune-far-16-millioner-kroner-i-statsstotte-etter-dataangrep-1.15776277 (Lastet ned 28.04.2023).

[11] SMB Norge. «Nasjonal sikkerhetsmyndighet: – Økt sikkerhetsrisiko for norske bedrifter.» DinBedrift.no. Hentet fra: https://dinbedrift.no/nasjonal-sikkerhetsmyndighet-okt-sikkerhetsrisiko-for-norske-bedrifter/ (Lastet ned 11.05.2023).

[12] Nasjonal sikkerhetsmyndighet, «Risiko 2023.» NSM, Oslo, Norge 13.02.2023. [Online]. Hentet fra: https://nsm.no/getfile.php/1312547-1676548301/NSM/Filer/Dokumenter/Rapporter/Risiko%202023%20-%20Nasjonal%20sikkerhetsmyndighet.pdf

[13] Nasjonal sikkerhetsmyndighet, *Leksjon 6 - Utvikling av grunnprinsippene*. (15.04.2020). Sett: Feb. 06. 2023. [Online video]. Hentet fra: https://ecourse.muniolms.com/en/user/course/5914/attempt/10422195/resource/15791/assets/eoX80utxNMKj5L27/story_content/video_5VfaZrdXf20_22_48_720x406.mp4

[14] Nasjonal sikkerhetsmyndighet. «Grunnprinsipper for IKT-sikkerhet.» NSM.no. Hentet fra: https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/grunnprinsipper-ikt (Lastet ned: 22.02.2023).

[15] Næringslivets Sikkerhetsråd, «Mørketallsundersøkelsen 2022.» Februar 2022. [Online] Hentet fra: https://www.nsr-org.no/produkter-og-tjenester/publikasjoner/morketallsundersokelsen (Lastet ned: 13.01.2023)

[16] Nasjonal sikkerhetsmyndighet. «Nasjonalt digitalt risikobilde 2021.» NSM, Oslo, Norge. 28.10.2021. Hentet fra: https://nsm.no/getfile.php/137495-1635323653/NSM/Filer/Dokumenter/Rapporter/NSM_IKT-risikobilde_2021_ny_B_enkeltside.pdf (Lastet ned: 25.04.2023).

[17] Departementene. «Småbedriftslivet - Strategi for små og mellomstore bedrifter.» Oslo, Norge. 04.10.2019. Hentet fra: https://www.regjeringen.no/globalassets/departementene/nfd/dokumenter/vedlegg/smabedriftslivet-uu.pdf (Lastet ned 19.05.2023).

[18] National Cyber Security Centre, «Small Business Guide: Cyber Security,» NCSC.gov.uk. Hentet fra: https://www.ncsc.gov.uk/collection/small-business-guide (Lastet ned: 30.03.2023).

[19] Nasjonal sikkerhetsmyndighet, «NSMs Grunnprinsipper for IKT-sikkerhet versjon 2.0.» Oslo, Norge. 15.04.2020. Hentet fra: https://nsm.no/getfile.php/133735-1592917067/NSM/Filer/Dokumenter/Veiledere/nsms-grunnprinsipper-for-ikt-sikkerhet-v2.0.pdf (Lastet ned: 24.01.2023).

[20] Nasjonal sikkerhetsmyndighet, «Støtteprodukter NSMs grunnprinsipper for IKT-sikkerhet.» Oslo, Norge. 03.07.2020. Hentet fra: https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/stotteprodukter/ (Lastet ned: 22.02.2023).

[21] *Informasjonsteknologi Sikringsteknikker Ledelsessystemer for informasjonssikkerhet Krav*, ISO/IEC 27001, 30.05.2017. [Online]. Hentet fra: https://standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=925900

[22] *Informasjonsteknologi Sikringsteknikker Ledelsessystemer for informasjonssikkerhet,* ISO/IEC 27002, 11.01.2013. [Online]. Hentet fra:

https://www.standard.no/no/nettbutikk/produktkatalogen/produktpresentasjon/?ProductID=665171

[23] National Institute of Standards and Technology, «Cybersecurity Framework - Getting started.» NIST.gov. Hentet fra: https://www.nist.gov/cyberframework/getting-started (Lastet ned: 07.04.2023).

[24] Center for Internet Security, «CIS Critical Security Controls.» Mai 2021. [Online]. Hentet fra: https://learn.cisecurity.org/cis-controls-download (Lastet ned: 20.04.2023).

[25] W. Chai, «What is the CIA triad (confidentiality, integrity and availability)?,» Techtarget.com. Hentet fra: https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA (Lastet ned 05.05.2023).

[26] H. Bergsjø, R. Windvik, L. Øverlier, *Digital sikkerhet en innføring*, Norge: Universitetsforlaget, 2020.

[27] Sjaak Laan, *It Infrastructure Architecture - Infrastructure Building Blocks and Concepts,* 3. utg. Morrisville, North Carolina, USA: Lulu.com, 2017.

[28] Digital Continuity Project, «Identifying Information Assets and Business Requirements.» England. 2011. Hentet fra: https://cdn.nationalarchives.gov.uk/documents/identify-information-assets.pdf (Lastet ned 23.03.2023).

[29] W. Curtis Preston, *Backup and Recovery*, Sebastopol, California, USA: O'Reilly Media, Inc, 2007.

[30] Microsoft. «Hva er løsepengevirus?.» Microsoft.no. Hentet fra: https://www.microsoft.com/nb-no/security/business/security-101/what-is-ransomware (Lastet ned: 23.03.2023).

[31] National Cyber Security Centre, «Offline backups in an online world,» NCSC.gov.uk. Hentet fra: https://www.ncsc.gov.uk/blog-post/offline-backups-in-an-online-world (Lastet ned: 05.05.2023).

[32] AXELOS. *ITIL Foundation,* 4. utg. England: The Stationary Office (TSO), 2019.

[33] Nasjonal sikkerhetsmyndighet. «Sikkerhetsfaglige anbefalinger ved tjenesteutsetting.» NSM.no. Hentet fra: https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/sikkerhetsfaglige-anbefalinger-ved-tjenesteutsetting/god-bestillerkompetanse/ (Lastet ned: 22.03.2023).

[34] C. M. Johansen, L. M. T. Sundbye. «Kvantitative og kvalitative metoder.» NDLA.no. Hentet fra: https://ndla.no/article/20755 (Lastet ned: 06.05.2023).

[35] Norges teknisk-naturvitenskapelige universitet. «Datainnsamling.» NTNU.no. Hentet fra: https://i.ntnu.no/wiki/-/wiki/Norsk/datainnsamling (Lastet ned: 02.02.2023).

[36] Universitet i Oslo. «Informasjonssikkerhet og risikovurdering for Nettskjema.» UIO.no. Hentet fra: https://www.uio.no/tjenester/it/adm-app/nettskjema/mer-om/informasjonssikkerhet/ (Lastet ned: 03.02.2023)

[37] National Institute of Standards and Technology. «Cybersecurity Framework version 1.1.» USA. 2018. Hentet fra: https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf (Lastet ned: 20.04.2023).

Vedlegg

Vedlegg 1: Informasjonsskriv

Vedlegg 2: Intervjuguide

Vedlegg 3: Flytdiagram for intervju

Vedlegg 4: Informantenes etterlevelse av prinsipp 2.9

Vedlegg 5: Innsalg av prosjektet

Vedlegg 1: Informasjonsskriv

Vil du delta i forskningsprosjektet

Virksomheters etterlevelse av NSMs grunnprinsipper for IKT-sikkerhet med fokus på sikkerhetskopieringspraksiser

Din innsikt og erfaring vil være svært verdifull for næringslivet og samfunnet for øvrig.

NTNU
Kunnskap for en bedre verden

Små og mellomstore bedrifter (SMB) blir stadig mer avhengig av informasjons- og kommunikasjonsteknologi (IKT) for å støtte sin virksomhet. Selv om disse bedriftene kanskje ikke har ressursene og ekspertisen til store organisasjoner når det gjelder IKT-sikkerhet, må de likevel ta dette på alvor for å beskytte sin kritiske forretningsinformasjon og systemer.

Cyberkriminelle retter stadig mer oppmerksomhet mot SMB som potensielle inngangsporter for å angripe større organisasjoner i leverandørkjedeangrep. I denne sammenhengen er det avgjørende at SMB forstår risikoen og tar hensiktsmessige tiltak for å beskytte seg mot cybertrusler. Dette forskningsprosjektet vil undersøke IKT-sikkerhet for SMB med særlig fokus på sikkerhetskopiering.

Formål

Formålet med denne oppgaven er å sette søkelys på hvor gode rutiner og prosesser små og mellomstore bedrifter har når det kommer til sikkerhetskopiering. Ved å ta utgangspunkt i et representativt antall bedrifter og sammenligne deres praksis med NSM sine anbefalinger for IKT-sikkerhet, vil vi finne ut hvor godt SMB er rustet for å motvirke sikkerhetshendelser som kan medføre datatap. Funn vi gjør vil bli brukt til å avdekke mulige løsninger for å øke etterlevelsen av NSMs anbefalinger for sikkerhetskopiering.

Problemstillingen vi besvarer er:

Hvordan kan man øke etterlevelsen til NSMs grunnprinsipper

for IKT-sikkerhet i forhold til sikkerhetskopiering?

Hvem er ansvarlig for forskningsprosjektet?

Norges Teknisk Naturvitenskapelige Universitet ved førstelektor Olav Skundberg er ansvarlig for prosjektet. Ekstern oppdragsgiver er Sopra Steria. Prosjektet gjennomføres av tre studenter tilhørende studieprogrammet Digital Infrastruktur og Cybersikkerhet.

Hvorfor får du spørsmål om å delta?

Du får spørsmål om å delta grunnet at du er ansatt i en bedrift der du har en grad av ansvar for IKT/sikkerhet. Vi har innhentet kontaktopplysningene dine fra offentlig tilgjengelig informasjon.

Hva innebærer det for deg å delta?

Hvis du velger å delta i dette prosjektet innebærer det at du deltar på et semistrukturert intervju. Det kommer til å bli tatt lydopptak av intervjuet, men dette lydopptaket vil ikke bli brukt til noe annet enn bacheloroppgaven, og all informasjon vil anonymiseres i forkant av publisering. Intervjuet vil ta ca. 15 - 30 minutter. Spørsmålene som blir stilt underveis i intervjuet vil være relatert til prosedyrer og tiltak når det gjelder sikkerhetskopiering av data. Et semistrukturert intervju innebærer at vi forbereder et sett med aktuelle spørsmål som vi ønsker svar på, og basert på svarene vil vi stille oppfølgingsspørsmål.

Det er frivillig å delta

Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykket tilbake uten å oppgi noen grunn. Alle dine personopplysninger vil da bli slettet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger

Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket.

- Studentene, veileder og oppdragsgiver vil ha tilgang til dataen som blir samlet inn.
- For å sikre at ingen uvedkommende får tilgang til dataen som blir lagret, vil vi lagre selve lydopptaket ett sted, mens bearbeidingen av dataen vil skje et annet sted. Lydopptaket vil bli lagret på Nettskjema, som er Norges sikreste og mest brukte løsning for datainnsamling til forskning og bearbeidingen av dataen vil skje i en kryptert mappe på OneDrive.

Hva skjer med personopplysningene dine når forskningsprosjektet avsluttes?

Prosjektet vil etter planen avsluttes 22. Mai 2023. Bacheloroppgaven vil være offentlig, men all informasjon som publiseres vil være anonymisert. Lydopptak anonymiseres ved transkribering og fjerning/endring av opplysninger som kan være identifiserende.

Når prosjektet er avsluttet vil lydopptak, transkribering og all bearbeiding av lydopptak bli slettet.

Hva gir oss rett til å behandle personopplysninger om deg?

Vi behandler opplysninger om deg hentet inn gjennom intervju basert på ditt samtykke. Innhenting av kontaktinformasjon om deg er basert på å utføre en oppgave i allmennhetens interesse.

Dine rettigheter

Så lenge du kan identifiseres i datamaterialet, har du rett til:

- Innsyn i hvilke opplysninger vi behandler om deg, og å få utlevert en kopi av opplysningene
- Å få rettet opplysninger om deg som er feil eller misvisende
- å få slettet personopplysninger om deg
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger

Hvis du har spørsmål til studien, eller ønsker å vite mer om eller benytte deg av dine rettigheter, ta kontakt med:

- NTNU ved prosjekveileder Olav Skundberg
    - E-post: olav.skundberg@ntnu.no
    - Telefon: 73 55 95 51.
- Student Fabian Hauge Sandvik
    - E-post: fabianhs@stud.ntnu.no
    - Telefon: 991 54 489
- NTNU ved personvernombud Thomas Helgesen
    - E-post: thomas.helgesen@ntnu.no
    - Telefon: 930 79 038

Hvis du har spørsmål knyttet til vurderingen som er gjort av personverntjenestene fra Sikt, kan du ta kontakt via:

- Epost: personverntjenester@sikt.no eller telefon: 73 98 40 40.

Med vennlig hilsen

Fabian Hauge Sandvik

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet *praktisk bruk av NSMs grunnprinsipper for IKT-sikkerhet* og har fått anledning til å stille spørsmål.

Jeg samtykker til:

- å delta i semistrukturert intervju

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet

---

(Signert av prosjektdeltaker, dato)

Vedlegg 2: Intervjuguide

Bacheloroppgave
ved
NTNU Digital Infrastruktur og Cybersikkerhet

Virksomheters etterlevelse av NSMs grunnprinsipper for IKT-sikkerhet med fokus på sikkerhetskopieringspraksiser

Innledning

Denne oppgaven har som mål å undersøke hvordan virksomheter gjennomfører sikkerhetskopiering av digitale verdier og sammenligne dette med anbefalingene fra Nasjonal Sikkerhetsmyndighet (NSM).

En av årsakene til at vi har valgt sikkerhetskopiering er at løsepengevirus er meget aktuelt for tiden og gode rutiner for sikkerhetskopiering er avgjørende for skadebegrensning.

Ettersom sikkerhetskopiering kan omfatte en rekke forskjellige verdier, og intervjuobjektene for dette prosjektet kommer fra ulike bransjer, vil det være viktig at du vurderer hvilke digitale verdier som du anser som virksomhetskritisk i din bedrift. Dette kan omfatte regnskap, kundedatabaser, digitale tegninger, programvare, og mye annet.

For virksomheter som har outsourcet IT-drift vil ikke alle spørsmålene være like relevante; vi vil justere hvilke spørsmål som stilles basert på svarene vi får. Vi vil ta hensyn til intervjuobjektenes bakgrunn og gi forklaringer på fagbegreper etter behov. Det er viktig å understreke at det ikke er noen krav til spesifikk kunnskap innenfor IKT-feltet for å delta i undersøkelsen.

Uavhengig av om sikkerhetskopiering gjennomføres internt eller av en tredjepartsleverandør vil hovedfokuset være på hvordan din bedrift praktiserer sikkerhetskopiering, og hvorvidt denne praksisen samsvarer med NSMs anbefalinger.

Kategori 0 – Intervjukandidatens ansvarsområder hos virksomhet

ID	Spørsmål
1	Hvilken stilling har du i virksomheten og hvor lenge har du hatt den?
2	Har du et overordnet ansvar for IKT-sikkerhet i stillingsbeskrivelsen din?
3	På en skala fra 1 til 10, hvor stort fokus mener du at din bedrift har på IKT-sikkerhet?

Kategori 1 – Overordnet IKT-sikkerhet hos virksomhet

ID	Spørsmål
4	Er virksomhetens IT-drift organisert ved at den er helt outsourcet, delvis outsourcet, eller er all drift organisert internt?
5	Følger dere et rammeverk for IKT-sikkerhet?
6	Har bedriften opplevd datatap som har fått økonomiske konsekvenser?
7	Hva slags digitale verdier anser dere som virksomhetskritisk for bedriften?
8	Har dere anslått hva det vil koste bedriften om virksomhetskritisk data blir utilgjengelig midlertidig eller permanent?

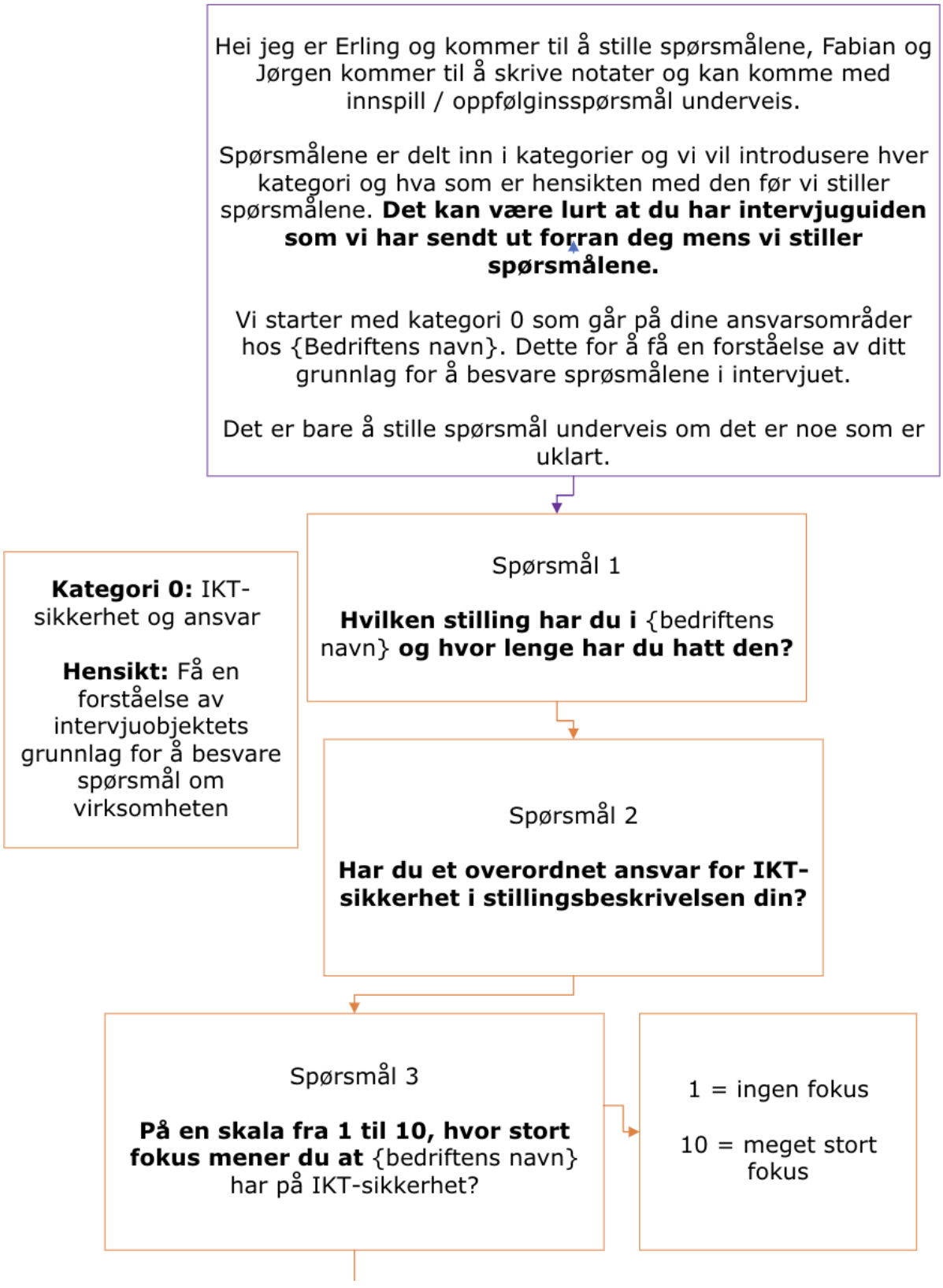
Kategori 2 – Etterlevelse av NSMs grunnprinsipper for IKT-sikkerhet, prinsipp *2.9 Etabler evne til gjenoppretting av data*

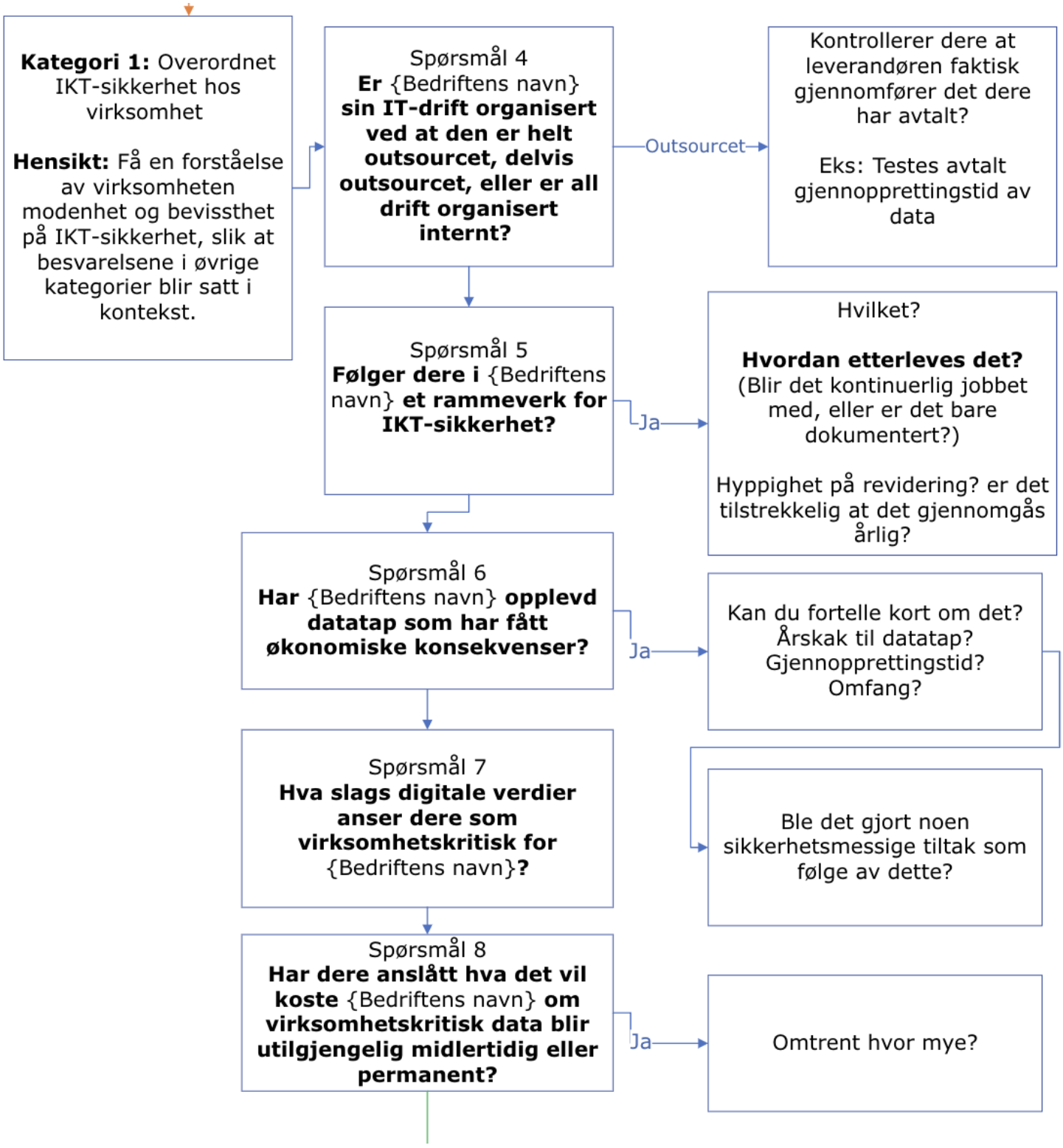
ID	Spørsmål
9	Har dere en plan for regelmessig sikkerhetskopiering av alle virksomhetsdata?
10	Har dere hatt noen utfordringer med å følge planen for sikkerhetskopiering?
11	Gjennomfører dere sikkerhetskopiering av programvare?
12	Utfører dere gjenopprettingstest regelmessig for å verifisere at sikkerhetskopien fungerer?
13	Hvordan beskyttes sikkerhetskopier mot tilsiktet og utilsiktet sletting, manipulering og avlesning?

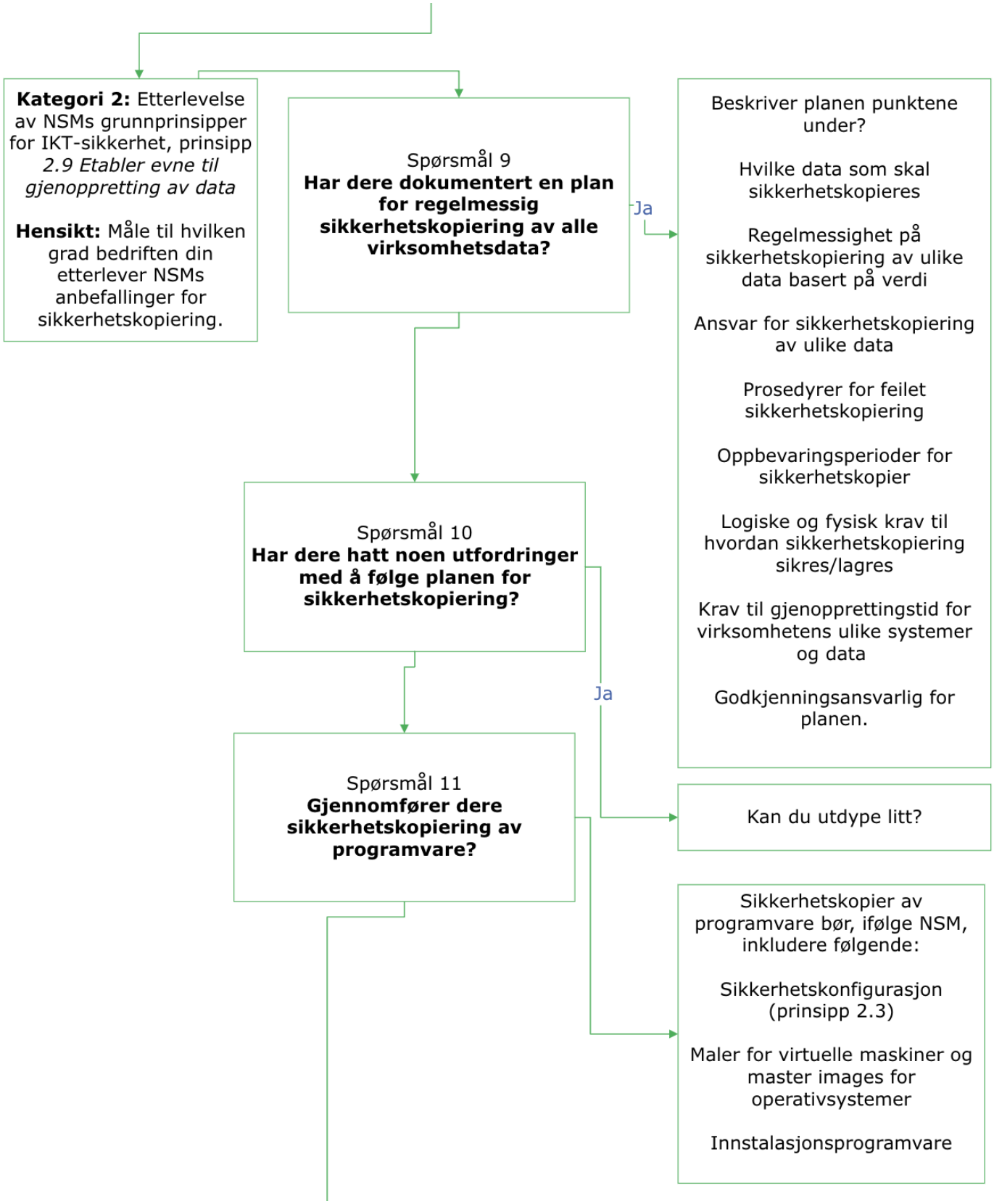
Kategori 3 – Utfordringer ved etterlevelse

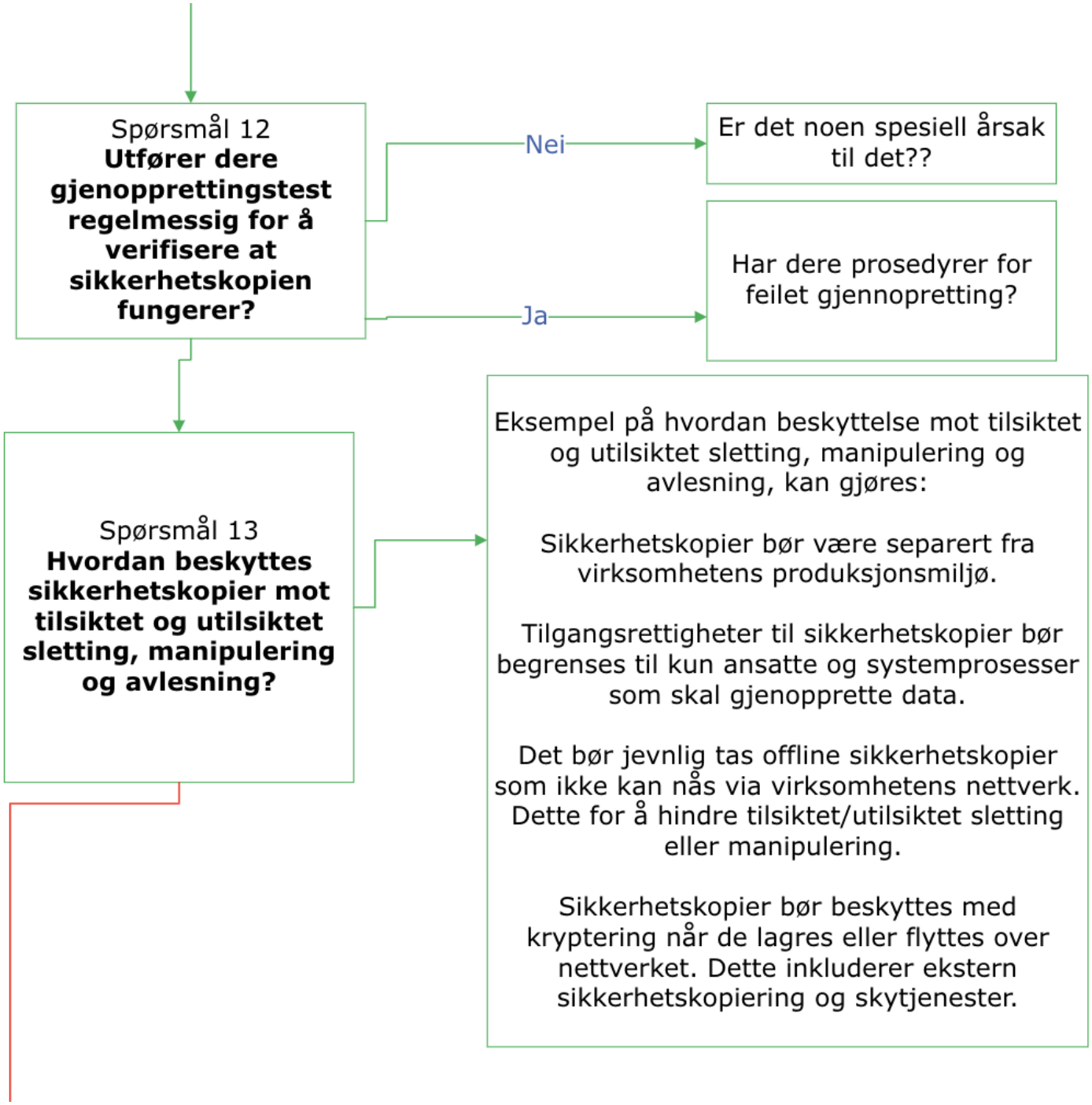
ID	Spørsmål
14	**Ledelse:** Syns du sikkerhetsarbeidet er godt forankret i ledelsen?
15	**Økonomi:** Får sikkerhetsarbeid tildelt tilstrekkelig med midler?
16	**Kompetanse og kapasitet:** Har ansatte med ansvar for IKT-sikkerhet tilstrekkelig kompetanse og kapasitet til å utføre arbeidet slik de anser det nødvendig?

Vedlegg 3: Flytdiagram for intervju

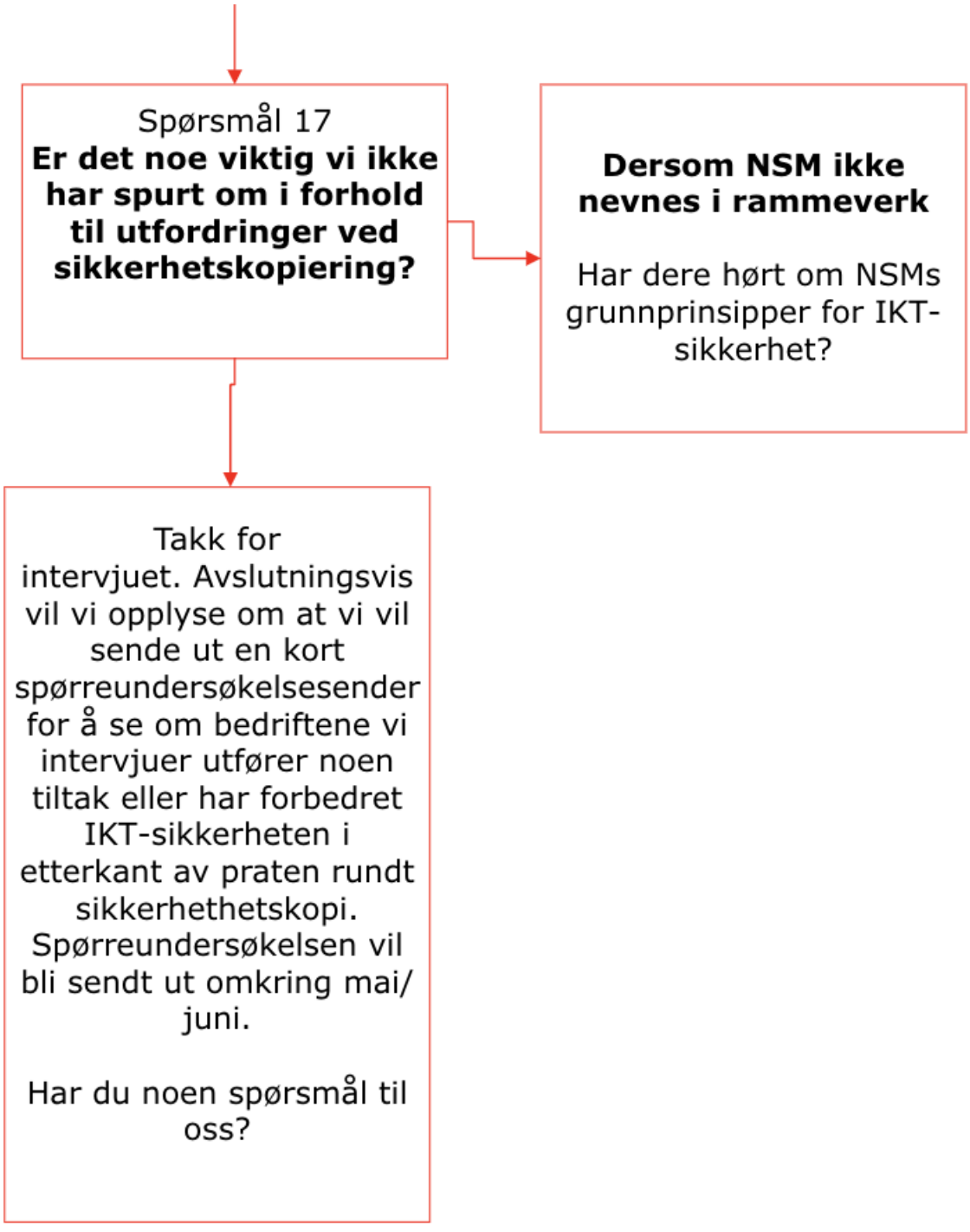



Kategori 1: Overordnet IKT-sikkerhet hos virksomhet
Hensikt: Få en forståelse av virksomheten modenhet og bevissthet på IKT-sikkerhet, slik at besvarelsene i øvrige kategorier blir satt i kontekst.
Spørsmål 4
Er {Bedriftens navn} **sin IT-drift organisert ved at den er helt outsourcet, delvis outsourcet, eller er all drift organisert internt?**
Outsourcet
Kontrollerer dere at leverandøren faktisk gjennomfører det dere har avtalt?
Eks: Testes avtalt gjennopprettingstid av data
Spørsmål 5
Følger dere i {Bedriftens navn} **et rammeverk for IKT-sikkerhet?**
Ja
Hvilket?
Hvordan etterleves det?
(Blir det kontinuerlig jobbet med, eller er det bare dokumentert?)
Hyppighet på revidering? er det tilstrekkelig at det gjennomgås årlig?
Spørsmål 6
Har {Bedriftens navn} **opplevd datatap som har fått økonomiske konsekvenser?**
Ja
Kan du fortelle kort om det?
Årskak til datatap?
Gjennopprettingstid?
Omfang?
Spørsmål 7
Hva slags digitale verdier anser dere som virksomhetskritisk for {Bedriftens navn}**?**
Ble det gjort noen sikkerhetsmessige tiltak som følge av dette?
Spørsmål 8
Har dere anslått hva det vil koste {Bedriftens navn} **om virksomhetskritisk data blir utilgjengelig midlertidig eller permanent?**
Ja
Omtrent hvor mye?


Kategori 2: Etterlevelse av NSMs grunnprinsipper for IKT-sikkerhet, prinsipp *2.9 Etabler evne til gjenoppretting av data*
Hensikt: Måle til hvilken grad bedriften din etterlever NSMs anbefallinger for sikkerhetskopiering.
Spørsmål 9
Har dere dokumentert en plan for regelmessig sikkerhetskopiering av alle virksomhetsdata?
Ja
Beskriver planen punktene under?
Hvilke data som skal sikkerhetskopieres
Regelmessighet på sikkerhetskopiering av ulike data basert på verdi
Ansvar for sikkerhetskopiering av ulike data
Prosedyrer for feilet sikkerhetskopiering
Oppbevaringsperioder for sikkerhetskopier
Logiske og fysisk krav til hvordan sikkerhetskopiering sikres/lagres
Krav til gjenopprettingstid for virksomhetens ulike systemer og data
Godkjenningsansvarlig for planen.
Spørsmål 10
Har dere hatt noen utfordringer med å følge planen for sikkerhetskopiering?
Ja
Kan du utdype litt?
Spørsmål 11
Gjennomfører dere sikkerhetskopiering av programvare?
Sikkerhetskopier av programvare bør, ifølge NSM, inkludere følgende:
Sikkerhetskonfigurasjon (prinsipp 2.3)
Maler for virtuelle maskiner og master images for operativsystemer
Innstalasjonsprogramvare


Spørsmål 12
Utfører dere gjenopprettingstest regelmessig for å verifisere at sikkerhetskopien fungerer?
Nei
Er det noen spesiell årsak til det??
Ja
Har dere prosedyrer for feilet gjennopretting?
Spørsmål 13
Hvordan beskyttes sikkerhetskopier mot tilsiktet og utilsiktet sletting, manipulering og avlesning?
Eksempel på hvordan beskyttelse mot tilsiktet og utilsiktet sletting, manipulering og avlesning, kan gjøres:
Sikkerhetskopier bør være separert fra virksomhetens produksjonsmiljø.
Tilgangsrettigheter til sikkerhetskopier bør begrenses til kun ansatte og systemprosesser som skal gjenopprette data.
Det bør jevnlig tas offline sikkerhetskopier som ikke kan nås via virksomhetens nettverk. Dette for å hindre tilsiktet/utilsiktet sletting eller manipulering.
Sikkerhetskopier bør beskyttes med kryptering når de lagres eller flyttes over nettverket. Dette inkluderer ekstern sikkerhetskopiering og skytjenester.


Hva mener du er den største utfordringen når det kommer til IKT-sikkerhetsarbeid i virksomheten?
Kategori 3: Utfordringer ved etterlevelse
Hensikt: Kartlegge utfordringer som intervjukandidaten i størst grad mener at påvirker IKT-sikkerhetsarbeidet i viksomheten.
Spørsmål 14
Syns du sikkerhetsarbeidet er godt forankret i ledelsen hos {Bedriftens navn}?
?
Har ledelsen godt nok fokus og tar ansvar for IKT-sikkerhet?
Spørsmål 15
Får sikkerhetsarbeid tildelt tilstrekkelig med midler?
Nei
Hva er årsaken til at det blir nedprioritert?
Spørsmål 16
Har ansatte med ansvar for IKT-sikkerhet tilstrekkelig kompetanse og kapasitet til å utføre arbeidet slik de anser det nødvendig?
Outsourcet
Betillerkompetanse
Har den som har ansvar for å bestille tjenester fra tredjepart tilstrekkelig kompetanse til å vite hva en skal bestille?
Manglende kompetanse?
Er grunnen til at det mangler kompetanse at det er mangel på kompetent personell i markedet?
(Her får vi vite om det blir nedrioritert, eller om det mangler kompetent personell)


Spørsmål 17
Er det noe viktig vi ikke har spurt om i forhold til utfordringer ved sikkerhetskopiering?
Dersom NSM ikke nevnes i rammeverk
Har dere hørt om NSMs grunnprinsipper for IKT-sikkerhet?
Takk for intervjuet. Avslutningsvis vil vi opplyse om at vi vil sende ut en kort spørreundersøkelsesender for å se om bedriftene vi intervjuer utfører noen tiltak eller har forbedret IKT-sikkerheten i etterkant av praten rundt sikkerhethetskopi. Spørreundersøkelsen vil bli sendt ut omkring mai/ juni.
Har du noen spørsmål til oss?

Vedlegg 4: Informantenes etterlevelse av prinsipp 2.9

Arkitekt 1			
Metrikk	**Besvarelse**	**Poeng**	**Begrunnelse**
Plan for sikkerhetskopi	Ja	4	
Antall punkter beskrevet i plan for sikkerhetskopi	5	10	
Sikkerhetskopi av programvare	Ja	5	Skyinfrastruktur og annet som gjør at de kan gjennopprette raskt ved behov
Testes gjenoppretting regelmessig	Nei	0	Kjørt gjenopprettinger ved behov
Oversikt over beskyttelse av sikkerhetskopi	Delvis	1	Tjenesteutsetter, men kan delvis svare på hvordan de beskytter sikkerhetskopiene
Antall punkter tilfredsstilt:	2	2	

CCO			
Metrikk	**Besvarelse**	**Poeng**	**Begrunnelse**
Plan for sikkerhetskopi	Ja	4	
Antall punkter beskrevet i plan for sikkerhetskopi	2	4	
Sikkerhetskopi av programvare	Ja	5	Sikkerhetskonfigurasjon
Testes gjenoppretting regelmessig	Nei	0	Kjørt gjenopprettinger ved behov, anser det som god nok testing
Oversikt over beskyttelse av sikkerhetskopi	God	1	«Leverandør tar seg av det»
Antall punkter tilfredsstilt:	4	4	

Sivilarkitekt			
Metrikk	**Besvarelse**	**Poeng**	**Begrunnelse**
Plan for sikkerhetskopi	Nei	0	Bedriften har ikke noen nedskreven plan over hvordan sikkerhetskopiering skal gjennomføres
Antall punkter beskrevet i plan for sikkerhetskopi		0	
Sikkerhetskopi av programvare	Har ikke behov	0	Sier at det ikke er inkludert da de går raskere å laste det ned fra nettet

Testes gjenoppretting regelmessig	Nei	0	Har testet én gang, gjøres ikke regelmessig
Oversikt over beskyttelse av sikkerhetskopi	Delvis	1	
Antall punkter tilfredsstilt	2	2	

IT-sjef			
Metrikk	**Besvarelse**	**Poeng**	**Begrunnelse**
Plan for sikkerhetskopi	Ja	4	
Antall punkter beskrevet i plan for sikkerhetskopi	4	8	
Sikkerhetskopi av programvare	Ja	5	
Testes gjenoppretting regelmessig	Nei	0	Har testet gjenoppretting, men dette gjøres ikke regelmessig
Oversikt over beskyttelse av sikkerhetskopi	God	1	
Antall punkter tilfredsstilt	4	4	

Daglig leder			
Metrikk	**Besvarelse**	**Poeng**	**Begrunnelse**
Plan for sikkerhetskopi	Ja	4	Planen er en del av et kvalitetssikringssystem
Antall punkter beskrevet i plan for sikkerhetskopi	3	6	
Sikkerhetskopi av programvare	Vet ikke	0	Antar det, men har ikke oversikt
Testes gjenoppretting regelmessig	Nei	0	
Oversikt over beskyttelse av sikkerhetskopi	Lite/ingen	0	Liten oversikt over tjenesteleverandørs praksis
Antall punkter tilfredsstilt	0	0	

Landskapsarkitekt 1			
Metrikk	**Besvarelse**	**Poeng**	**Begrunnelse**
Plan for sikkerhetskopi	Ja	4	Har en plan som er utarbeidet av tredjepart
Antall punkter beskrevet i plan for sikkerhetskopi	5	10	
Sikkerhetskopi av programvare	Ja	5	Serverbilder
Testes gjenoppretting regelmessig	Nei	0	Tredjepart har lovet at dette skal inngå i

			tjenesten, men er ikke blitt utført
Oversikt over beskyttelse av sikkerhetskopi	Delvis	1	
Antall punkter tilfredsstilt	3	3	

CTO			
Metrikk	**Besvarelse**	**Poeng**	**Begrunnelse**
Plan for sikkerhetskopi	Nei	0	Har ikke en plan
Antall punkter beskrevet i plan for sikkerhetskopi	0	0	
Sikkerhetskopi av programvare	Ja	5	Noe sikkerhetskopiert på fysiske maskiner og noe i Git
Testes gjenoppretting regelmessig	Nei	0	
Oversikt over beskyttelse av sikkerhetskopi	God	1	
Antall punkter tilfredsstilt	3	3	

Arkitekt 2			
Metrikk	**Besvarelse**	**Poeng**	**Begrunnelse**
Plan for sikkerhetskopi	Nei	0	Har utarbeidet en rutine i samarbeid med leverandør, men ikke noe skriftlig
Antall punkter beskrevet i plan for sikkerhetskopi	0	0	
Sikkerhetskopi av programvare	Nei	0	Mener de ikke har behov
Testes gjenoppretting regelmessig	Nei	0	Ikke regelmessig
Oversikt over beskyttelse av sikkerhetskopi	Delvis	1	
Antall punkter tilfredsstilt	1	1	

CISO			
Metrikk	**Besvarelse**	**Poeng**	**Begrunnelse**
Plan for sikkerhetskopi	Ja	4	
Antall punkter beskrevet i plan for sikkerhetskopi	8	16	Full uttelling, har en utfyllende plan
Sikkerhetskopi av programvare	Nei	0	Foreløpig ikke behov, men ved at det kan komme
Testes gjenoppretting regelmessig	Nei	0	Har ikke gjort det enda, men planlegger det

Oversikt over beskyttelse av sikkerhetskopi	God	1	
Antall punkter tilfredsstilt	3	3	

Landskapsarkitekt 2			
Metrikk	**Besvarelse**	**Poeng**	**Begrunnelse**
Plan for sikkerhetskopi	Nei	0	Ingen plan utover regler i sikkerhetskopierings software
Antall punkter beskrevet i plan for sikkerhetskopi	0	0	
Sikkerhetskopi av programvare	Nei	0	
Testes gjenoppretting regelmessig	Nei	0	Gjorde det før, men ikke lenger
Oversikt over beskyttelse av sikkerhetskopi	Delvis	1	
Antall punkter tilfredsstilt	1	1	

Partner			
Metrikk	**Besvarelse**	**Poeng**	**Begrunnelse**
Plan for sikkerhetskopi	Nei	0	Har ikke prioritert det
Antall punkter beskrevet i plan for sikkerhetskopi	0	0	
Sikkerhetskopi av programvare	Nei	0	
Testes gjenoppretting regelmessig	Nei	0	
Oversikt over beskyttelse av sikkerhetskopi	Lite/ingen	0	
Antall punkter tilfredsstilt	0	0	

Vedlegg 5: Innsalg av prosjektet

Hei!

Vil du være med på et forskningsprosjekt om IKT-sikkerhet?

Vi er studenter ved NTNU som skriver vår bacheloroppgave om praktisk bruk av NSMs grunnprinsipper for IKT-sikkerhet. Vi ønsker å bidra til å øke bevissthet rundt IKT-sikkerhetsutfordringer ved å undersøke hva som gjør det utfordrende for små og mellomstore bedrifter å etterleve grunnprinsippene.

For å gjøre dette trenger vi å snakke med ansatte i små og mellomstore bedrifter om deres erfaringer og utfordringer når det gjelder IKT-sikkerhet. Vi tror at deres innsikt vil være nyttig for å forstå hva som gjør det utfordrende for bedrifter å etterleve NSMs grunnprinsipper, og hva som kan gjøres for å forbedre situasjonen.

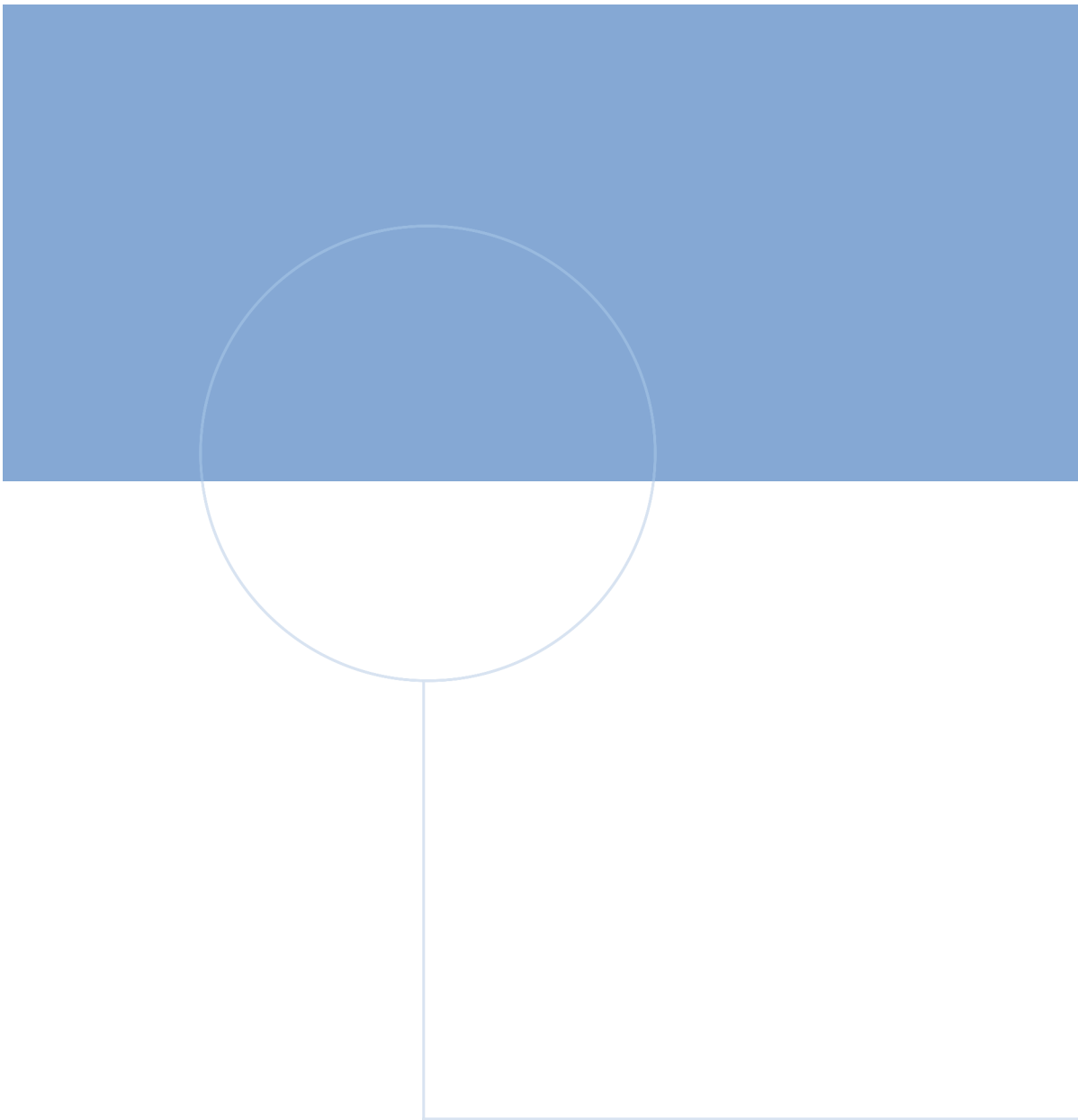
Ved å delta i intervjuet vil du bidra til å gi oss en bedre forståelse av utfordringene ved å etterleve NSMs grunnprinsipper for IKT-sikkerhet. Samtidig vil du også bidra til å øke kunnskapen om IKT-sikkerhet i din egen bedrift og i bransjen generelt. Dersom dere ønsker det, kan vi avslutningsvis gi dere en innføring i rammeverket til NSM for IKT-sikkerhet.

Vi ønsker å gjennomføre intervjuer med ansvarlige for IT- og sikkerhet i en bedrift. Erfaring med NSMs grunnprinsipper for IKT-sikkerhet er ikke et krav. Vi garanterer at alle opplysninger du gir oss vil bli behandlet konfidensielt og vil ikke bli brukt til noe annet formål enn vår bacheloroppgave.

Takk for at du tar deg tid til å lese denne meldingen. Om det kan være aktuelt for deg og din bedrift å delta, eller du kjenner noen som kan være interessert – ta kontakt med oss på fabianhs@stud.ntnu.no for en uforpliktende prat.

Med vennlig hilsen,

Fabian H Sandvik, Erling C Fladvad & Jørgen T Nilsen



NTNU

Kunnskap for en bedre verden