Phishingangrep i oljesektoren

En studie av hvordan oljeselskaper arbeider for å redusere risikoen for phishingangrep mot sine ansatte.

Elisabeth Fossmark

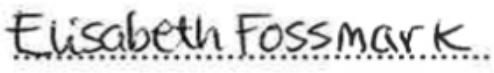
Masteroppgave 2020

Oppgaven er innlevert som en del av mastergradsstudiet i samfunnssikkerhet ved Universitetet i Stavanger.

Universitetet i Stavanger

DET TEKNISK-NATURVITENSKAPELIGE FAKULTET

MASTEROPPGAVE

Studieprogram/spesialisering: Master i samfunnssikkerhet	Vårsemesteret, 2020 Åpen
Forfatter: Elisabeth Fossmark	 *(Signatur forfatter)*
Fagansvarlig: Ole Andreas Hegland Engen **Veileder:** Henrik Kvadsheim	
Tittel på masteroppgaven: Phishingangrep i oljesektoren – En studie av hvordan oljeselskaper arbeider for å redusere risikoen for phishingangrep mot sine ansatte. **Engelsk tittel:** Phishing attacks in the oil sector – A study of how oil companies work to reduce the risk of phishing attacks on their employees.	
Studiepoeng: 30	
Emneord: Cyber security, IKT-sikkerhet, oljesektor, phishingangrep, nyansatte, policy og rutiner, risikopersepsjon, sikkerhetskultur, etablerte ansatte, kunnskap og kompetanse.	Sidetall: 80 + vedlegg/annet: 83 Oslo, 12.juni 2020

Forside for masteroppgaven

Det Teknisk-naturvitenskapelige fakultet

Forord

Denne masteroppgaven markerer min siste etappe som student ved Universitetet i Stavanger. Arbeidet med masteroppgaven har vært lærerikt, spennende og krevende. I tillegg har oppgaven bidratt til etterlengtet kunnskap om cybersikkerhet og digitaliseringens sårbarheter. Kunnskapen jeg har tilegnet meg gjennom oppgaven er både viktig og dagsaktuell i et stadig mer digitalisert samfunn.

En stor takk rettes til alle informantene som selv under spesielle omstendigheter kunne stille til intervju og bidro til at oppgaven ble mulig å gjennomføre. Kunnskapen og ærligheten dere bragte til oppgaven settes stor pris på!

Takk til veileder Henrik Kvadsheim, for tett oppfølging, raske tilbakemeldinger og gode veiledninger.

En stor takk går til mine foreldre for å ha motivert og støttet meg gjennom hele masterstudiet. Sist men ikke minst, takk til min samboer Erlend. Takk for at du setter krav, bryr deg og hele tiden oppmuntrer meg til å prestere best mulig.

Elisabeth Fossmark, 12.Juni 2020.

Sammendrag

Den norske oljesektoren har gjennomgått store digitale forandringer fra 1960-tallet og frem til i dag. Teknologiske revolusjoner gjør at vi kan produsere olje og gass på helt nye måter. Digitaliseringen og teknologifokuset i oljesektoren bidrar til å gjøre oljeindustrien mer effektiv og skånsom enn tidligere. Samtidig kommer en ikke unna at teknologien og digitaliseringen også fører med seg sårbarheter. Blant sårbarhetene er angrepsmetoder via internett en stor trussel for oljesektoren. I denne oppgaven fokuseres det på phishing som en cybertrussel, som gjennom oppgaven har utpekt seg som den cybertrusselen oljeselskapene ser absolutt mest av. Et phishingangrep gjennomføres ved at en ondsinnet aktør sender en e-post med et infisert vedlegg til ansatte i et selskap. Formålet er å skade eller ta nytte av selskapets verdier.

Videre fokuserer oppgaven på i hvilken grad nyansatte kan utgjøre en større risiko for phishingangrep enn etablerte ansatte. I starten av et arbeidsforhold er nyansatte hverken kjent med selskapets policys, rutiner eller sikkerhetskultur. Det er fraværet av disse faktorene som kan gjøre en nyansatt mer sårbar for phishingangrep i starten av arbeidsforholdet. Hensikten med oppgaven er å studere i hvilken grad phishingangrep er en større trussel for nyansatte, hvilket la grunnlaget for følgende problemstilling:

I hvilken grad utgjør nyansatte en større risiko for phishingangrep enn etablerte ansatte i oljesektoren?

For å svare på problemstillingen ble det gjennom en kvalitativ metode gjennomført både intervjuer og dokumentstudier. Funnene viser at oljeselskapene har et høyt fokus på phishingangrep som en trussel. Selskapene jobber kontinuerlig med bedring av kurs og phishingkampanjer for å øke ansattes kunnskap og kompetanse om phishing. Informantintervjuene viste også at selskapene jobber med kunnskap- og kompetanseheving på ulike måter og av ulik kvalitet. Når det kommer til phishingangrep mot nyansatte viser funnene at selv om nyansatte ofte er yngre med god teknologiforståelse utgjør de likevel en risiko i starten av arbeidsforholdet. Ønske om å gjøre et godt inntrykk i samspill med å ikke være godt kjent med selskapets policys og rutiner er faktorer som bidrar til at en nyansatt kan uten vilje bli offer for et phishingangrep.

Figurer:

Tabeller:

Forkortelser:

HRO – High Reliability Organizations
NHO – Næringslivets Hovedorganisasjon
NorSIS – Norsk Senter for Informasjonssikkerhet
NOROG – Norsk olje&gass
NOU – Norsk Offentlig Utredning
NSM – Nasjonal Sikkerhetsmyndighet
NSR – Næringslivets Sikkerhetsråd
PST – Politiets Sikkerhetstjeneste
Ptil – Petroleumstilsynet

1.0 Innledning

1.1 Bakgrunn

Tidligere samfunnssikkerhetsminister Ingvil Smines Tybring-Gjedde sa i januar 2020 at kriminaliteten har gått fra gata, til data (Midsec, 2020). I Politiets Sikkerhetstjeneste sin sikkerhetsvurdering for 2020 kommer digital kartlegging og sabotasje av kritisk infrastruktur frem som en av de mest alvorlige truslene Norge står over i det kommende året (Politiets Sikkerhetstjeneste [PST], 2020). Videre forklarer PST (2020) at store deler av trusselaktiviteten foregår i det digitale rom. Norge har blitt et komplekst, avhengig og digitalt samfunn, dette gir også økt sårbarhet og mulighet for ondsinnede aktører til å gjennomføre spionasje, manipulasjon og sabotasje. Digitaliseringen gir oss mange goder, men det er også med på å gjøre oss sårbare for cybertrusler (Norsk Offentlig Utredning [NOU] 2015:13).

En kjent og ofte brukt cybertrussel er E-postangrep. E-post er en etablert kommunikasjonskanal som vi bruker både privat og i jobbsammenheng. Et e-postangrep innebærer å samle inn sensitiv informasjon, drive svindel eller å infisere datamaskiner gjennom ondsinnede linker, koder eller vedlegg (PwC, 2019). Disse angrepene blir ofte betegnet som phishingangrep og ordet phishing kommer fra å fiske informasjon fra andre. Storebrand skriver at phishingangrep er den største trusselen mot digital sikkerhet (Storebrand, u.å). Norsk senter for Informasjonssikring skriver i sin artikkel at phishing er den mest effektive metoden for å kapre en brukerkonto (Norsk senter for Informasjonssikkerhet [NorSIS], 2017). November 2019 sa også sjefen for Europol sitt Europeiske Cybercrimesenter at phishing er en metode som gir mulighet for noen av de mest alvorlige formene for nettkriminalitet. Videre sier han at phishingangrep kan forårsake reell skade for både europeiske borgere og organisasjoner (Europol, 2019).

Phishing er ikke en ny angrepsmetode, men den er fremdeles en av de mest brukte angrepsmetodene. Antall registrerte phishingangrep økte fra 8% i 2016 til 18% i 2018 (Næringslivets Sikkerhetsråd, 2018). Ifølge Cisco (2018) begynner angrepene å vise tendenser til å bli mer målrettet mot nyansatte. PwC (2019) skriver i tillegg at ansatte og deres ubeviste handlinger er den største trusselen mot selskapers IT-sikkerhet. Nyansatte bruker sine første uker i ny jobb til å få tilgang på nye systemer, gjennomgå opplæring og skape bekjentskap med nye kollegaer. I innkjøringsperioden får nyansatte tilsendt store mengder informasjon og

et øyeblikks uoppmerksomhet bidra til at den nyansatte blir offer for et phishingangrep. Mailer om kontonummer for lønn, brukernavn og passord kan virke mer naturlig grunnet innkjøringsperioden og de nyansatte kan lettere bli lurt av en phishingmail. Svindlerne kan på denne måten enklere få suksess i forsøkene på å fiske ut ønsket informasjon. Som nyansatt er en ikke kjent med selskapets rutiner eller policys, dette er faktorer som kan bidra til å gjøre de nyansatte ekstra sårbare for phishingangrep (Cisco, 2018).

En sektor som har opplevd flere phishingangrep er oljesektoren. Oljesektoren har flere verdier som kan være attraktive mål for ondsinnede aktører og årsakene til angrepene er mange. Blant annet store økonomiske vinninger, tap av omdømme, sensitiv informasjon og sabotasje. Eksempelvis sitter oljeselskapene på sensitiv informasjon om leting og boring som kan være av interesse hos både nasjonale og internasjonale aktører (Regjeringen, 2015-2016). I tillegg bidrar økt automatisering, flere tilkoblinger til datanettverk og økning i bruken av skylagring til at oljesektoren er mer eksponert for cyberangrep. Oljenæringen med dens kompleksitet og avhengighet gir gjennom økt sårbarhet også muligheten for ondsinnede aktører til å gjennomføre spionasje, manipulasjon og sabotasje. Revolusjonerende teknologiske løsninger, datadeling og sammenkobling av systemer gir oljebransjen flere fordeler, men det bidrar også til økt sårbarhet (Petroleumstilsynet [Ptil], 2019).

1.2 Problemstilling

Politiets sikkerhetstjeneste, Nasjonal sikkerhetsmyndighet, Politiet og Næringslivets Sikkerhetsråd skriver i sin felles veileder «*Sikkerhet ved ansettelsesforhold*» (2017) at i dagens arbeidsliv er det flere og flere som blir midlertidig ansatt, enten på kontrakt, som konsulent eller kontraktør. Selv om lengden på ansettelsesforholdet varierer blir de vist samme tillit som andre fast ansatte i selskapet. Kunnskap og tillit i kombinasjon gjør at den nyansatte kan enten med overlegg, eller uten vilje, skade bedriften. Skader uten vilje kan oppstå ved at den nyansatte ikke forstår rutinene og verdiene i bedriften. Eksempel på dette kan være phishingangrep. Gjennom phishingangrep kan den nyansatte skape konsekvenser for bedriften i form av økonomisk tap, eksponering av sensitiv informasjon, svekket omdømme eller tap av forretningshemmeligheter (PST, 2017). I denne oppgaven er formålet å se på hvorvidt nyansatte utgjør en risiko for å bli utsatt for phishingangrep i oljesektoren. En sektor som er kjent for å være profesjonelle aktører med et høyt aktsomhetsnivå (Regjeringen, 2018). I lys av innledningen og informasjonen over har jeg kommet frem til følgende

problemstilling:

I hvilken grad utgjør nyansatte en større risiko for phishingangrep enn etablerte ansatte i oljesektoren?

For å besvare problemstillingen er det utarbeidet tre forskningsspørsmål:

1. Hvordan har oljesektoren erkjent og forholdt seg til phishing som en cybertrussel, og i hvilken grad har en fokuset på nyansatte som sårbar gruppe i forhold til denne trusselen?

Forskningsspørsmålet forsøker å svare på hvor kjent phishingangrep er for oljesektoren og i hvilken grad de anerkjenner det som en trussel for oljeselskapet og deres verdier. Det gjennomgås videre hvilke cybertrusler oljeselskaper i Norge står ovenfor i dag. Forskningsspørsmålet fokuserer i tillegg på i hvilken grad oljeselskapene tar høyde for at nyansatte kan utgjør en større risiko for phishingangrep i begynnelsen av arbeidsforholdet.

2. Hvorfor og hvordan spiller kunnskap og kompetanse inn på de ansattes forståelse av phishingangrep?

I dette forskningsspørsmålet legges det vekt på i hvor stor grad kunnskap og kompetanse kan utgjøre en forskjell for ansatte i møtet med et phishingangrep. NorSIS forklarer at kunnskap og opplæring kan redusere sjansen for cyberangrep. Jo mer kunnskap vi har om fenomenet, jo større er sjansen for at vi sikrer oss på en bedre måte. Ved å gjøre tiltak som å iverksette en totrinnsbekreftelse, oppdatere programvarer og antivirusbeskyttelse samtidig som vi er mer bevisste på hvilke digitale spor vi legger igjen, vil sikkerheten kunne forbedres (NorSIS, 2020). For at disse tiltakene faktisk blir gjennomført vil det være viktig med kunnskap, kompetanse og opplæring. FuseMail skriver at kunnskapen og bevisstheten til de ansatte er en suksessfaktor i møtet med phishingangrep. Ved å heve hele organisasjonens kunnskapsnivå om phishingangrep vil du samtidig heve beskyttelsesnivået til selskapet (FuseMail, 2017). Forskningsspørsmålet tar utgangspunkt i både NorSIS og FuseMail og forsøker å svare på i hvilken grad kunnskap- og kompetanseheving blir praktisert av oljeselskapene. I tillegg forsøker forskningsspørsmålet å belyse hvordan kunnskap og kompetanse kan bidra positivt til å redusere risikoen for at ansatte blir utsatt for et phishingangrep.

3. Hvordan kan oljesektoren arbeide for å redusere risikoen for at ansatte blir utsatt for et phishingangrep?

I det siste forskningsspørsmålet søker jeg å finne svar på hvilke arbeidsmetoder som kan på best mulig måte bidra til å redusere risikoen for phishingangrep. Gjennom forskningsspørsmålet blir det presentert hvordan selskapene arbeider med phishingangrep i dag og hvordan endring av metoder og fremgangsmåter kan bidra til å styrke selskapet i møtet med phishingangrep i fremtiden.

Avgrensning

Tid og kapasitet nødvendiggjør avgrensninger i denne oppgaven. Omfanget av ulike cybertrusler som kan ramme norsk oljesektor er stort og det er ikke mulig å ta for seg hele trusselbildet. På bakgrunn av dette var det beste for oppgaven å fordype seg i en spesifikk cybertrussel, nemlig phishingangrep. Valget om å fokusere på denne cybertrusselen kommer av at det stadig fokuseres på og advares mot phishingangrep som en angrepsmetode. Likevel finnes det lite forskning på nyansatte og hvor utsatt de er for phishingangrep i en oppstartsperiode. Av empirisk innsamling vil fokuset være på utvalgte oljeselskaper, med det formål om å gi et overordnet bilde av arbeidet oljesektoren gjør for å hindre phishingangrep mot sine ansatte.

1.3 Faglig relevans

Digitalisering og dens påvirkning av norsk oljenæring bidrar til bedre, enklere og mindre ressurskrevende løsninger. Samtidig bringer det også med seg en risiko for uønskede handlinger i form av cyberangrep. Vi kan lære av å se på hvilke cybermetoder som har blitt brukt og på denne måten være bedre rustet i fremtiden. Gjennom arbeidet med oppgaven har det vært fremtredende at phishing er den mest brukte metoden. Det å gå i dybden på hvorfor og hvordan nyansatte blir målskiver for phishingangrep vil kunne avdekke noen sårbarheter og hvordan en kan dimensjonere seg opp mot denne trusselen. Det finnes flere rapporter og avhandlinger om phishing som fenomen, som i tillegg viser den enorme skaden det kan ha for selskapets verdier. Denne oppgaven vil se på arbeidet selskapene etablerer i forkant av et angrep, rettet mot nyansatte, og hvordan selskapene på best mulig kan redusere risikoen for angrep. På bakgrunn av dette vil oppgaven bidra til videre forskning mot tematikken som

studien forsker på. Den faglige relevansen vil bli belyst gjennom bruk av teori fra samfunnssikkerhetstudiet med særlig med fokus på sikkerhetskultur, kunnskap og kompetanse.

1.4 Tidligere forskning

I følge VadeSecure (2019) er nyansatte det perfekte mål for et phishingangrep. Det begrunnes med at nyansatte er lite kjent med både folk og prosess i sitt nye arbeidsforhold. Dette gjør at nyansatte kan være mer sårbare for phishingangrep. Det begrunnes med at de ikke er kjent med sikkerhetskulturen eller prosessen i sin nye arbeidshverdag. I tillegg trekker VadeSecure (2019) frem at nyansatte ønsker å gi et godt inntrykk og frykter for å gjøre feil. I et phishingangrep kan ønsket om å svare raskt på henvendelser gjøre at den nyansatte overser kjennetegnene ved en phishingmail og dermed blir lurt (VadeSecure, 2019). Atea (2018) skriver på sin blogg at cyberangrep mot bedrifter øker, samtidig som angrepene blir mer sofistikerte og farlige. En ny vinkling er å rette angrepene mot nyansatte. Dette forklarer Atea ved at nyansatte møter opp hos sin nye arbeidsgiver klar for å bruke sine første uker på å blant annet få tilganger, bli kjent med ansatte og få opplæring. Det er også i disse første ukene at de nyansatte er på sitt mest sårbare. Videre forklarer Atea at grunnen til at nyansatte er mer utsatt er på grunn av at de ikke kjenner til selskapets prosesser i tillegg til at du overdøves av mail fra både HR, overordnede og kollegaer. Mailene inneholder blant annet lenker med applikasjoner og systemer som må lastet ned, dokumenter som må leses og opplæringsvideoer som må ses. Det er i dette kaoset av mailer at en god hacker kan ense sin mulighet (Atea, 2018).

Sikkerhets- og beredskapsarbeidet er et lederansvar, men det påvirker likevel alle nivåer i bedriften. Derfor er det viktig at arbeidet prioriteres og at tiltakene er allment kjent og forstått både for nyansatte, etablerte ansatte og ledere (Nasjonal sikkerhetsmyndighet, 2015). Det rettes særlig fokus mot phishing som en metode for cyberangrep, som er en av de vanligste og største truslene (Næringslivets Sikkerhetsråd [NSR], 2018). Politiets sikkerhetstjeneste, Nasjonal sikkerhetsmyndighet, Politiet og Næringslivets Sikkerhetsråd skriver også som nevnt i *1.2 Problemstilling* i sin veileder at nyansatte blir vist samme tillit som etablerte ansatte og at dette kan bidra til at de nyansatte uten vilje kan skade selskapet gjennom eksempelvis et phishingangrep (2017).

PwC sin Cybercrime Survey fra 2019 viser at ansatte og deres ubevisste handlinger er en stor

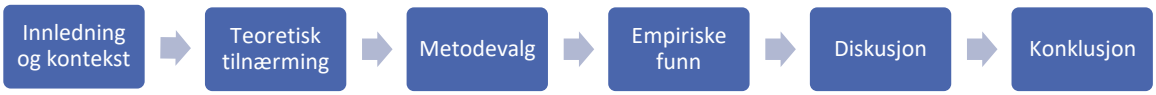
trussel. Phishingangrep er blant de hyppigste angrepsformene og hele 84% av respondentene i undersøkelsen hadde opplevd et slikt angrep. En positiv utvikling er at på den andre siden oppgir 53% at bevisstgjøring av ansatte er en høyt prioritert sikkerhetsinnvestering i tiden fremover (PwC, 2019). Ifølge PRO ISP er falske e-poster en av de største sikkerhetstruslene mot både privatpersoner og bedrifter på nett. I tillegg opplyser de om at 80% ikke klarer å identifisere om mailen de har mottatt er et phishingforsøk eller ikke (PRO ISP, 2018). Red Level hadde en studie i 2018 der det kom frem at av 500.000.000 e-poster var 1 av hver 101 e-post skadelig. Videre forklarer Red Level at den største risikoen i hvert selskap er personene som jobber der. Et trykk av et individ på en ondsinnet link er alt som skal til, og hele selskapet kan bli infisert av et skadelig virus (Red Level, 2019).

SecurityInnovation (u.å) skriver at ofte får teknologien skylden for cyberangrep selv om menneskelig feil er årsaken 52% av gangene. Generelt sett er det mennesker som bruker teknologien, uvitende om de teknologiske sårbarhetene. Dette gir en gyllen mulighet for hackerne til å komme seg inn i systemene. De fleste selskaper tror at teknologiske løsninger som brannvegg og anti-virus programmer er nok til å kunne hindre et angrep. Dessverre kan ingen teknologi gjøre rede for menneskelige feil og uaktsomhet. Selv om teknologi kan ha tillatt angrepet å skje, er det mennesket som er ansvarlig for angrepet. Derfor er opplæring i sikkerhetsbevissthet viktig. Bevisstheten har økt de siste årene, ettersom flere selskaper blir mål for sikkerhetsbrudd. Likevel viser de til at hele 46% av selskaper ikke har noen form for opplæring i sikkerhetsbevissthet. Og selv om selskaper faktisk driver sikkerhetsopplæring er det fremdeles mange som faller tilbake på dårlige vaner ved å eksempelvis trykke på lenker i uønskede e-poster (SecurityInnovation, u.å).

Som nevnt i *1.2 Problemstilling* skriver NorSIS at ved å gjøre tiltak som å iverksette en totrinnsbekreftelse, oppdatere programvarer og antivirusbeskyttelse samtidig som vi er mer bevisste på hvilke digitale spor vi legger igjen, vil sikkerheten kunne forbedres (NorSIS, 2020). Nettvett (2019) ramser i tillegg opp flere forholdsregler som kan bidra til å minske sannsynligheten for et phishingangrep. Blant annet fokus på å sjekke skrivefeil i både e-postadressen til avsender og nettsiden du blir henvist til. Her er det gode muligheter til å oppdage at adressene er forfalsket og på denne måten kan phishingforsøket avsløres. Videre poengterer Nettvett (2019) at en aldri skal sende personlig informasjon eller bankkontodetaljer over e-post. Et annet godt tips er å hele tiden oppdatere PC-en og programmene samtidig som du til enhver tid benytter deg av antivirusprogrammer. Microsoft

(u.å) kommer med flere av de samme anbefalingene. Samtidig poengterer de viktigheten av å ha nok kunnskap. Kunnskap om hvordan du beskytter deg fra et phishingangrep vil være et av de sterkeste barrierene. PRO IPS (2018) skriver at phishing er et økende problem i tillegg til at angrepene blir mer og mer avanserte og målrettede. Av forholdsregler nevner PRO IPS (2018) mye av det samme som nevnt tidligere, men de avslutter med å oppfordre folk til å være skeptiske til e-poster som kommer i innboksen. Dersom du er usikker skal du la være å åpne e-posten.

1.5 Oppgavens struktur



Figur 1: Oppgavens oppbygning (Eget arbeid, 2020).

I første del av oppgaven presenteres bakgrunn for valg av tema og oppgave, tidligere forskning, presentasjon av problemstilling og forskningsspørsmål, avgrensning, begrepsavklaring og kontekst.

Andre del av oppgaven tar for seg den teoretiske tilnærmingen. Her vil det gjennomgås relevant teori knyttet opp mot forskningsspørsmålene.

I oppgavens tredje del vil den metodiske tilnærmingen legges frem. Her forklares og begrunnes forskningsdesign, metodiske valg, datatype og datainnsamling. Tilslutt i del tre gjennomgås det etiske refleksjoner samt drøfting av metodens styrker og svakheter. Del fire er en gjennomgang av empiriske funn fra datainnsamlingen.

Oppgavens del fem tar for seg empirien satt opp mot teorien. I denne delen vil det vurderes og diskuteres om eksisterende teori kan forklare de empiriske funnene gjort i oppgaven.

Tilslutt i oppgaven vil konklusjonen legges frem ved å svare på problemstilling og forskningsspørsmål. I den siste delen av oppgaven fremlegges også forslag og anbefalinger til videre forskning.

2.0 Avgrensning og kontekst

I dette kapittelet vil konteksten for oppgaven legges frem. I avgrensningen vil jeg gå nærmere inn på begrepene digitalisering, IKT-sikkerhet, cybersikkerhet og cyberangrep. Samtidig blir forskjellen mellom begrepene «safety» og «security» belyst. Deretter redegjør jeg for phishingangrep, hva det er, hvordan det brukes og hvilken metode av phishingangrep som blir brukt mot nyansatte. I konteksten utdypes videre oljesektoren og dens digitaliseringsprosess, samt hvorfor oljesektoren er relevant som avgrensning i oppgaven når det kommer til phishingangrep mot nyansatte.

Digitalisering

100 år med økende vekst i datakraft har ført til den tredje industrielle revolusjonen, også kalt den digitale. Store og hyppige teknologiske endringer gjør at både mennesker og organisasjoner vil ha vanskeligheter med å forestille seg og begripe hvilke konsekvenser det kan føre med seg (PwC, u.å). Digitalisering har og vil endre både det norske samfunn, næringen og arbeidslivet i fremtiden. Blant annet vil nye varer og tjenester bli produsert og brukt mer effektivt enn før. Nye inntekst- og forretningsmodeller blir utviklet og bidrar til å redusere kostnader og priser (Næringslivets Hovedorganisasjon [NHO], 2018). Bare på en uke blir det produsert mer data enn i løpet av hele forrige årtusen (Meld. St. 27, 2015-2016). Disse nye teknologiene fører også med seg endringer som kan utfordre hele samfunnet (NHO, 2018).

IKT-sikkerhet og cybersikkerhet

IKT-sikkerhet viser til evnen til å fremme nettverk som er sikre, robuste og stabile (Meld. St. 38, 2016-2017). IKT står for informasjons- og kommunikasjonsteknologi (Store Norske Leksikon [SNL], 2019). IKT-sikkerhet skal i all hovedsak sikre informasjon på tre forskjellige måter. Sikre konfidensialitet, sikre integritet og sikre tilgjengelighet ved behov. Informasjonssikkerhet kan til dels overlappe med IKT-sikkerhet, da informasjonssikkerhet omhandler sikring av både digital og ikke-digital informasjon (Digitaliseringsdirektoratet, u.å). Informasjonssikkerhet og IKT-sikkerhet er helt nødvendig for å kunne ivareta digitaliseringen og teknologiske løsninger på best mulig måte. Det gjøres gjennom oppdaterte trussel- og sårbarhetsvurderinger for å holde følge med den digitale utviklingen.

Det er en fin linje mellom IKT-sikkerhet og cybersikkerhet. Ifølge Regjeringen, PST og NSM ligger cybersikkerhet som en underkategori hos IKT-sikkerhet. Forskjellen er at IKT-sikkerhet rommer et mer generelt og bredt spekter av farer og trusler, mens cybersikkerhet er mer rettet mot samfunnssikkerhet (Regjeringen, 2010). På den andre siden skrives det i NOU 2015:13 at cybersikkerhet er synonymt med IKT-sikkerhet (NOU, 2015:13). Enkelt forklart kan en si at cybersikkerhet omhandler tiltak for å beskytte trusler som kan komme gjennom en IKT-infrastruktur (Regjeringen, 2010). Det som gjør cybersikkerhet utfordrende er at det finnes flere digitale enheter enn mennesker i en bedrift samtidig som at angriperne blir dyktigere og mer innovative. Samfunnet er avhengig av kritisk infrastruktur og dermed blir sikringen av disse avgjørende for at samfunnet skal fungere (Cisco, u.å).

«Safety» og «Security»

Ved ondsinnede og villede handlinger er en opptatt av sikring. I et engelsk ordforråd vil sikringsbegrepet ligge mellom «safety» og «security» (Lindøe, 2018). I Norge har vi derimot bare et begrep, nemlig sikkerhet, som skal representere både «safety» og «security» (SINTEF INFOSEC, 2016). En forenklet beskrivelse av forskjellen er at «security» kan forstås som evnen til å sikre seg mot tilsiktede uønskede handlinger, som phishingangrep, mens «safety» betyr å sikre seg mot uhell, ulykker eller tilfeldige uønskede handlinger, som skogbrann (Stranden, 2019). Innen IKT-sikkerhet («IKT-security») er hovedmålet å beskytte konfidensialitet, integritet og tilgjengelighet av informasjon, mens «safety» har som mål å beskytte liv, helse eller miljø mot skader. «Security» fokuserer på trusler fra utenfor systemet, ofte forårsaket av ondsinnede handlinger, mens «safety» fokuserer på utilsiktede handlinger. Disse forskjellene resulterer i forskjellige grunnlag for hvilke tiltak og barrierer som bør iverksettes (Bartnes, 2006).

I denne oppgaven vil «security» være det mest passende begrepet å bruke, da phishingangrep kan kategoriseres som en tilsiktet handling. «Security» henger tett sammen med sikring. PST, NSM og Politidirektoratet definerer sikring som bruken av tiltak for å håndtere risiko i møte med tilsiktede handlinger (2015). Sikring mot phishingangrep skal redusere eller motstå konsekvensene av handlingene som bevisst er påført organisasjonen gjennom teknologi (Engen et al., 2016). Forskjellen på «Security» og «Safety» er viktig å legge frem for å videre kunne forstå meningen bak begrepet cyber security som blir brukt i denne oppgaven.

Cyberangrep

Cyberangrep blir beskrevet som en trussel som kommer utenfra med det formål om å skade, forstyrre eller overbelaste systemer. Et godt eksempel på et slikt cyberangrep er phishing. I et phishingangrep åpner en ansatt en ondsinnet lenke eller et infisert vedlegg fra en e-post. Handlingen fører til at det aktiveres et ondsinnet program eller at en uønsket aktør får tilgang til selskapets systemer. Konsekvensene kan være at PC-en som lenken ble åpnet på slutter å virke, data spres eller systemer stopper opp. Dette kan få alvorlige følger for det selskapet som blir rammet (NHO, 2018).

To av de mest omtalte cyberangrepene i vår tid er Wannacry og NotPetaya. WannaCry var et løspengevirus som spredde seg internasjonalt gjennom datamaskiner som brukte en eldre versjon av Windows. Ifølge Financial Times startet det hele med at en person åpnet et ondsinnet vedlegg i en e-post (NRK, 2017). NotPetaya var en utpressingsvare som blant annet rammet Maersk og kostet dem minst 1,9 milliarder danske kroner (Digi, 2018). Et annet kjent angrep er angrepet mot kraftsektoren i Ukraina i desember 2016. Her klarte hackerne å skru av strømmen i hovedstaden Kiev i underkant av en time. Skadevaren har fått navnet «Industroyer» og den har egenskaper til å kunne gjøre skade på store industrielle kontrollsystemer (NorSIS, 2017).

I følge NorSIS sin rapport om trusler og trender for 2019-2020 er følgende cyberangrep de ti største digitale truslene for Norge og norske selskaper:

Trussel	Beskrivelse
Phishing	Kriminelle lurer deg til å oppgi sensitiv informasjon, enten om deg selv eller selskapet du jobber i. Phishingangrep skjer ofte gjennom en ondsinnet link i en e-post.
Løspengevirus	Viruset krypterer filer på datamaskinen din og krever løsepenger for å frigjøre dem.
ID-tyveri	Noen utgir seg for å være deg og bruker din ID til å logge seg inn i systemer, en konto eller gir tilganger.

Falske trusler og utpressingskrav	Det kan eksempelvis være pornosvindel. Du får en e-post om at noen har filmet deg mens du så på porno. For å ikke «lekke» filmen krever de penger av deg.
Ekte utpressing og svindel	Seksuell utpressing, datingsvindel, direktørsvindel, fakturasvindel, investeringsbedrageri eller telefonsvindel.
Kontohacking	Noen hacker kontoen din, enten det er Facebook-, Instagram- eller mailkonto. Hackere tar over kontoen og kan bruke den som de vil.
Menneskelig feil	NSM utga i 2018 en mørketallsundersøkelse, denne viste at mer enn halvparten av sikkerhetsbrudd skyldes menneskelig feil.
Datainnbrudd	Datainnbrudd eller hacking vil si at en person som i utgangspunktet er uten tilgang klarer å gjøre innbrudd i systemer som gjør at de får tilgang.
Krenkelser	Mobbing, trakassering, trusler og hets som via nett blir sendt til enkeltpersoner, grupper eller virksomheter.
Verdikjedeangrep	Gjennom å angripe underleverandører eller mer usikre enheter klarer hackere å komme seg inn i en virksomhet. De går da ikke direkte på virksomheten, men gjennom det svakeste leddet (NorSIS, 2020).

Tabell 1: Ti største digitale trusler for Norge (NorSIS, 2020).

Formålet til cybersikkerhet og IKT-sikkerhet er å komme med tiltak som kan hindre et cyberangrep. For phishingangrep kan gode tiltak eksempelvis være brannmurer som hindrer angripere å komme seg inn i systemene eller at ansatte velger sterke passord til sine

brukernavn.

Phishingangrep

Phishing blir direkte oversatt til norsk som nettfiske og er en kjent metode for svindlere. Typisk skjer det gjennom e-post hvor mottaker oppfordres til å legge igjen personlig informasjon som eksempelvis kontoinformasjon eller påloggingsinformasjon (Digi, 2015). Et eksempel er Hilary Clinton sin tidligere kampanjeleder John Podesta. Han ble utsatt for et phisingangrep i 2016. Det startet med at han fikk en e-post fra noen som utga seg for å være Google. I e-posten sto det at passordet hans var blitt eksponert og at passordet måtte endres. Podesta skrev da inn det gamle passordet og lagte et nytt. På denne måten fikk hackerne tilgang til brukeren hans og tabben var et faktum (CBS News, 2016).

E-posten som blir sendt ut ser ofte ut som de kommer fra pålitelige kilder, samtidig som de har en beskjed eller avtale som det haster å få svar på (Uninett, 2013). På denne måten får svindlerne informasjonen de trenger for å gjennomføre angrepet. Ifølge NSM lar vi oss ofte lure av disse e-postene. For en trusselaktører holder det at kun én person blir lurt. Når trusselaktøren først har kommet seg inn i systemet kan de begynne å utvide tilgangen (NSM, 2020).

Phishingangrep foregår ofte gjennom fire faser. Første fase er rekognosering, dette gjøres for å gjennomføre et så målrettet angrep som mulig. For hackere vil dette innebære å undersøke sosiale medier, i dette tilfelle er LinkedIn det perfekte verktøyet for å finne nyansatte. Andre fase er distribusjon, det er selve phishingmailen som blir sendt ut til alle ansatte i et oljeselskap. Med små grep, som å ha et legitimt utseende med for eksempel firmalogo og påfølgende «*Velkommen til vårt firma*» tekst, vil terskelen være lav for at nyansatte trykker på den ondsinnede lenken eller vedlegget. Distribusjonen kan også gjennomføres ved å skape frykt, eksempelvis å skrive at dersom innloggingsdetaljer ikke fylles inn i skjemaet vil brukeren bli låst. Fase tre omhandler selve spredningen. Når angriperne har kommet seg inn i systemet starter de med å spre angrepet, stjele data og låse systemer. Dette fører tilslutt over på den fjerde og siste fasen som er utbetaling. Hackerne krever utbetaling enten for at du skal få systemene dine tilbake, for å hindre at de skal spre sensitiv informasjon eller for å hindre ødeleggelse av system (Cisco, 2018).

Figur 2: Fasene i phishingangrep (Eget arbeid, 2020).

Det finnes flere typer phishingangrep, noen er svært målrettet, noen er rettet mot enkeltpersoner og noen foregår kun over telefon eller via sosiale medier. I denne oppgaven fokuseres det på den mest populære metoden som er generelle phishingangrep som sendes ut til flere mennesker, hvor målet er at en skal trykke på en ondsinnet link. Et typisk utseende for en slik e-post ser gjerne slik ut:


RE: Tusen takk

DA DIAKITE Alexandre <a.diakite@agglo-pau.fr>
Til DIAKITE Alexandre

Svar | Svar til alle | Videresend

I dag, mandag 2. mars 2020, oppdaterer vi e-postsystemet vårt til Microsoft Outlook Web App 2020. Denne tjenesten skaper mer plass og enkel tilgang til e-post. Oppdater kontoen din ved å klikke på lenken nedenfor og skriv inn aktiveringsinformasjonen.

Klikk for å aktivere, klikk her.

Hvis du ikke klarer å fullføre informasjonen, blir kontoen din inaktiv.

Tusen takk.
Konsulentsenter, (@) 2020. Alle rettigheter forbeholdt.

Eksempel på phishingmail (Fra egen e-post, 2020).

Eksempelet over er hentet fra min egen arbeidsgiver. I mailen blir ansatte oppfordret til å trykke på en link for å aktivere en ny oppdatering. I tillegg kommer det en advarsel om at kontoen din vil bli inaktiv dersom du ikke klarer å fullføre informasjonen. Oppgaven ser i hovedsak på hvordan nyansatte utgjør en større risiko for å trykke på linker som eksempelvis denne. I følgende delkapittel vil det redegjøres for hvorfor oljesektoren er en interessant og relevant sektor å fokusere på når det kommer til phishingangrep.

2.1 Oljesektoren og digitalisering

Den internasjonale omsetningen til norske oljeserviceselskaper i 2017 var på omtrent 100 milliarder NOK. I 2018 bidro Norsk petroleumsnæring med cirka 286 milliarder NOK til staten (Norsk olje og gass [NOROG], 2019). I tillegg anslås det at norsk petroleumsnæring gir

staten netto kontantstrøm på 238 milliarder NOK for 2019 og netto kontantstrøm på 245 milliarder NOK for 2020 (Norsk Petroleum, 2020). På Kapital sin oversikt over Norges 500 største selskaper i 2017 er det 11 olje- og gass selskaper inne de 100 største, tilsammen omsetter de for 571,89 milliarder NOK. Til sammenligning har bank og finans også 11 selskaper innen de 100 største og omsetter for 319,86 milliarder NOK (Kapital, u.å). Disse tallene viser at i oljesektoren er det store økonomiske verdier, både for den norske stat, men også for oljeselskapene selv.

Teknologien i norsk oljesektor har gjennomgått store forandringer fra slutten av 1960-tallet og frem til i dag. Bruken av både små og store teknologiske revolusjoner gjør at vi i dag kan produsere olje og gass på nye måter. Eksempelvis blir enkelte prosesser på plattformer styrt fra land. Teknologien bidrar til å finne effektive løsninger på hvordan man kan finne, bygge ut og produsere olje og gass på en god måte som også er skånsom for miljø og klima (Norsk Petroleum, 2019). Petroleumsforskning og teknologi koster penger. Nedturen oljenæringen opplevde i 2014-2018 ga et høyt fokus på kostnadsreduksjon. Blant annet ønsker mange å redusere antall manuelle operasjoner eller skyve arbeidet fra offshore til onshore (PwC, u.å.). Gjennom økt fokus og ønske om et bedre og mer optimalisert produksjonspotensial er digitalisering et av de viktigste virkemidlene (Gressgård, L.J., Melberg, K., Risdal, M., Selvik, J.T., Skotnes, R.Ø, 2018). Under ONS 2018 i Stavanger var det en egen utstillingsavdeling for bedrifter som tilbyr digitale løsninger for olje- og gassindustrien (Sysla, 2018). Kostnadsfokuset til oljenæringen gjør at digitale løsninger blir en hovedkomponent til kostnadsgevinster.

Oljesektoren er kjent for store datamengder, bruk av teknologi og digitale innovasjoner. Selv om digitaliseringen bidrar positivt til næringen er cyberangrep mot norske olje- og gasselskaper en reell trussel. I 2010 skrev Nasjonal Sikkerhetsmyndighet i sin rapport om sikkerhetstilstanden at angrepsmetoder via internett er en stor trussel (Nasjonal sikkerhetsmyndighet [NSM], 2010). To år etterpå, i 2012 ble et av de største oljeselskapene i verden angrepet gjennom et cyberangrep. Saudi Aramco ble utsatt for et dataangrepet kalt Shamoon. De stjal de ansattes passord, slettet dokumenter og e-poster samt titusenvis av selskapets dataservere ble gjort ubrukelige (Trend Micro, 2019). Målet til angriperne var å stoppe olje- og gassproduksjonen til Saudi Armaco, som står for 10% av den globale oljeforsyningen (Reuters, 2020).

Maersk ble som nevnt tidligere utsatt for et globalt cyberangrep kalt NotPetya. Flere ansatte samlet seg hos selskapets IT-avdeling for råd. På enkelte PC-skjermer sto det meldinger med sterk advarsel om å ikke skru av datamaskinen. Andre PC-skjermer hadde tekstbokser hvor det sto at filene var kryptert og det ville koste 300 dollar i Bitcoins for å dekryptere filene (Wired, 2018). Flere IT-systemer ble angrepet i tillegg til utvalgte forretningsenheter (Maersk, 2017). Angrepet endte opp med å koste shippingselskapet tilsammen 300.000.000 dollar (Wired, 2018). I 2019 ble også Norsk Hydro utsatt for et omfattende cyberangrep ved navnet LockerGoga (NHO, 2019). LockerGoga opererer ved å få tilgang til en PC og deretter går fra PC til PC for å stjele passord som tilslutt gir tilgang lengre opp i systemet (E24, 2019). Angrepet påvirket Hydro globalt, og resultatet var store operasjonelle utfordringer og økonomiske tap. Selskapet måtte over til manuell drift for å kunne opprettholde noe av driften. Totalt har de estimert at kostnaden for angrepet var på cirka 500-600 millioner NOK (Hydro, 2019).

NSM sendte også i 2015 ut en advarsel til olje- og energisektoren om at det vil komme forsøk på dataangrep. I etterkant av varselet ble det avdekket over 50 forsøk på dataangrep i sektoren. Angrepene var hovedsakelig e-poster med ondsinnede vedlegg, og dersom de ble åpnet ville skadevaren kunne implementere seg i systemet (NSM, 2015). Oljenæringen har tidligere opplevd cyberangrep og den nye forskningsrapporten til Trend
Micro advarer også mot kommende angrep (Trend Micro, 2019) Prognosene har i tillegg vist at oljesektoren planla å begynne ansette igjen i tiden fremover. Noe som i utgangspunktet vil bety at oljesektoren i fremtiden vil ha mange nyansatte. Etter nedgangen oljeselskapene opplevde mellom 2014-2018 har de begynt å utlyse stillinger igjen (Norsk Petroleum, 2020). En fersk rapport fra DNV GL skriver at flere ledere i oljebransjen planla og ansatte flere i løpet av 2019 (Teknisk Ukeblad, 2019). Også ifølge forskningsinstituttet IRIS ville det fra 2018-2020 bli rundt 22.000 nye ansatte i olje- og gass sektoren (Enerwe, 2016).

Disse forutsetningene viste seg å ikke stemme. Viruset Covid-19 (heretter kalt «Corona») ble oppdaget i Kina i november 2019 og den 26.02.2020 ble viruset oppdaget i Norge (NRK, 2020). I tillegg til å påvirke liv, helse, arbeidsplasser og økonomi har viruset også påvirket oljesektoren. Blant annet førte det til en priskrig mellom Saudi-Arabia og Russland. Dette bidro til at etterspørselen etter olje falt kraftig (Finansavisen, 2020). Dagens Næringsliv skrev 26.mars at oljefondets coronatap var på 1330 milliarder kroner, på størrelsen med et norsk statsbudsjett (DN, 2020). Samtidig gikk Nasjonal Sikkerhetsmyndighet ut i mars og varslet

om at kriminelle utnytter situasjonen ved å utføre digitale angrep og svindel på nett. Også i NSM sin risikovurdering for 2020 gir de uttrykk for at økt bruk av hjemmekontor fører med seg ulike digitale sårbarheter og trusler (NSM, 2020). Typiske angrep er phishingangrep med tema knyttet til Corona utbruddet. Enormt mange personer har hjemmekontor på grunn av Corona, noe som bidrar til et helt nytt digitalt trusselbilde for norske virksomheter (Digi, 2020). På hjemmekontor er IKT-sikkerheten ansett som lavere enn om du er på arbeidsplassen. Flere sikkerhetsselskaper meldte om en økning i phishingangrep hvor svindlerne bevisst utnytter situasjonen Corona har satt oss i (NSM, 2020).

Dette delkapittelet viser at oljesektoren er en sektor som kan kunne oppleve nye angrep i fremtiden, og i aller høyeste grad er aktuelle som grunnlag for å si noe om phishingangrep mot både nyansatte og etablerte ansatte. Selv om ansettelsen av nye arbeidstakere må vente på seg på grunn av Corona, vil nok oljenæringen på sikt begynne å ansette igjen. Gjennom økt digitalisering og høyt teknologisk tempo er oljesektoren en sektor med flere positive trender, men med den teknologiske utviklingen følger også potensielle konsekvenser. Som nevnt tidligere er eksempler på konsekvenser for oljeselskapene økonomisk tap, svekket omdømme eller spredning og manipulering av informasjon. Et vellykket phishingangrep kan også få større konsekvenser enn de nevnte. Plattformer består av industrielle kontrollsystem som jobber med tungt utstyr, væske som kan ta fyr og arbeid under høyt trykk, havner disse kontrollsystemene i feil hender kan menneskeliv gå tapt (Høydal, 2020).

3.0 Teori

For å kunne svare på problemstillingen og følgende forskningsspørsmål vil teori om risiko kunne bidra til å forklare hvorfor phishingangrep utgjør sikkerhetsrisiko for et oljeselskap. Videre vil teori om risikopersepsjon si noe om hvordan de ansatte opplever risikoen og hvordan et selskap kan endre oppfatningen gjennom økt kompetanse. Dette gjøres ved hjelp av teoriene om kunnskap, læring og opplæring. Tilslutt vil teori om sikkerhetskultur og samhandlingen mellom menneske, teknologi og organisasjon være betydningsfulle for å kunne diskutere hvordan selskapene best mulig kan arbeide for å hindre trusselen som phishing utgjør for sine ansatte. I teorikapittelet vil det bli lagt frem ulike teorier som sammen danner et grunnlag for å kunne svare på oppgavens forskningsspørsmål med tilhørende problemstilling.

3.1 Risiko

For oljesektoren er det stor risiko knyttet til den økende digitaliseringen. Begrepet risiko kan forstås som en uønsket hendelse. Risiko er noe som inntreffer, enten av naturlige årsaker som for eksempel vulkanutbrudd eller som følge av planlagte og ikke-planlagte hendelser fra mennesker, eksempelvis brann på oljeplattform eller phishingangrep (Engen et al., 2016). Risiko knyttet til tilsiktede uønskede handlinger skiller seg fra ulykker og utilsiktede handlinger på flere områder. Mest sentralt er det faktum at det dreier seg om tre faktorer og ikke bare to. Ved ulykker og utilsiktede handlinger handler det om sannsynlighet og konsekvens, mens for tilsiktede handlinger handler det om trussel, sårbarhet og verdi. Det kan være bort imot umulig å regne seg frem til sannsynligheten for en tilsiktet handling, spesielt sjeldne hendelser. Risiko står ikke alene, men må ses sammen med en spesiell aktivitet eller av en eksistens (Stranden, 2019). I denne oppgaven vil risiko ses i sammenheng med phishingangrep som en uønsket handling.

Verdier, trusler og sårbarhet er begreper som er sentrale innenfor risiko (Bergsjø, Windvik & Øverlier, 2020). Oljesektoren har flere verdier som en ondsinnet aktør kan ønske å skade. For oljeselskaper kan en verdi eksempelvis være sensitiv informasjon. Det finnes mye informasjon som ikke bør komme ut til ondsinnede aktører som omhandler blant annet letefasen, feltutvikling, produksjon og transport av olje og gass. Andre eksempler på verdier for oljesektoren er liv, helse, økonomi og omdømme. Trussel viser til de kriminelle aktørenes

evne, kapasitet og vilje til å utføre et phishingangrep, mens sårbarheten viser til sikkerhetshull som gjør at angrepet blir vellykket. Denne fremgangsmåten er lik alle tilsiktede uønskede hendelser (NOU 2015:13).

Risikobegrepet er interessant i forbindelse med hvordan informantene forstår cybertrusler som en risiko, og hvor stor grad av oppmerksomhet selskapet retter mot den spesifikke risikoen. Samtidig vil risiko og forståelsen av risiko si noe om hvordan de arbeider med phishingangrep i det aktuelle oljeselskapet. Den risikoen som får oppmerksomhet og som selskapet forstår konsekvensene av får ofte en sentral rolle i sikkerhetsarbeidet. Dersom phishing blir forstått som en stor risiko med høy grad av uønskede konsekvenser vil også arbeidet med å hindre et phishingangrep bli et fokusområde hos selskapene.

3.1.1 Risikopersepsjon

I risikopersepsjon legges menneskets subjektive oppfattelse av risiko til grunne, altså hvordan risikoen blir opplevd og forstått av den enkelte. Risikovurderingene påvirkes av verdier, holdninger, erfaringer og egenskaper som mennesket besitter (Engen et al., 2016). For en nyansatt vil den risikopersepsjonen de besitter i starten av ansettelsesforholdet være viktig for selskapet. Dersom den ansatte kjenner til og forstår phishing som en trussel vil det påvirke risikopersepsjonen i form av kunnskap om fenomenet. Dette vil styrke både den nyansatte og selskapet i møtet med et phishingangrep. Hva den individuelle oppfatter som risiko og hvor risikofylt det oppleves er styrt både av individet men også kulturen individet er en del av (Boyesen, 2003). Dermed har selskapet også en forpliktelse til å arbeide med den ansattes risikopersepsjon slik at det blir en sterkere felles risikoforståelse.

Oljeselskapers forebyggende arbeid spiller inn på hvordan de ansatte opplever risikoen. I oppgaven legges det vekt på hvordan nyansatte og etablerte ansatte gjennom kunnskap og kompetanse fra selskapets og dens sikkerhetskultur bidrar til å minske risikoen for et phishingangrep. Aven og Renn (2010) skriver omtrent det samme i sin forklaring av risikopersepsjon, nemlig at risikopersepsjon ligger i enkeltindividets egne vurderinger og oppfattelser av risiko. Disse vurderingene og oppfattelsene har lett for å være påvirket av fryktfaktorer, vitenskapelig risikovurderinger, personlige verdier og fakta. Risikopersepsjonen sier noe om menneskers risikoforståelse (Boyesen, 2003). I oppgaven vil risikopersepsjon bidra til å belyse i hvilken grad oljeselskapene ser på nyansatte som en større risiko eller ikke.

Samtidig vil risikopersepsjon ses igjen i hvordan opplæringen til de ulike selskapene fungerer. Dersom de ansatte får god opplæring, med sterkt fokus på kunnskap og kompetanse vil dette bidra positivt til de ansattes risikopersepsjon. Noe som igjen bidrar til å høyne sikkerhetsnivået i selskapet.

3.2 Kunnskap, kompetanse, læring og opplæring

3.2.1 Fra informasjon til kunnskap og kompetanse

For at oljeselselskapene skal kunne redusere sjansen for at deres ansatte går på et phishingangrep vil det være viktig at de ansatte har opparbeidet seg kunnskap og kompetanse. Dersom en har kunnskap og kompetanse om phishing som fenomen og de konsekvensene det innebærer vil de ansatte lettere kunne gjenkjenne et phishingforsøk og rapportere det inn. Alle selskaper er, og vil i fremtiden, være avhengig av å etablere kunnskap og kompetanse for å lykkes i å nå sine visjoner og mål. Naisbitt (1982) skriver «*Vi drukner i informasjon, men tørster etter kunnskap» (s.32).* Det er viktig å skille informasjon fra kunnskap, det er ikke slik at om de ansatte får informasjon så utvikler de kunnskap. Informasjon forblir informasjon når den ikke anvendes gjennom handling, mens informasjon som anvendes gjennom handling gir kunnskap og kompetanse (Filstad, 2010).

En skiller mellom kunnskap, informasjon, data og viten. Data er tall og informasjon blir tolkingen av disse dataene. Informasjonen blir som nevnt kun til kunnskap når den anvendes gjennom erfaring og forståelse. I et oljeselskap kan dette eksempelvis være data og informasjon om antall forsøk på phishingangrep eller konsekvensene av et phishingangrep. For de ansatte vil dette kun være informasjon frem til de får anvende informasjonen gjennom handling, eksempelvis kurs eller opplæring. Utviklingen fra informasjon til kunnskap krever dermed at både kropp og hjerne tas i bruk. Interaksjon og refleksjon vil derfor være helt avgjørende (Filstad, 2010).

Videre blir kunnskap utviklet til kompetanse gjennom de ansattes deltakelse i ulike praksisfellesskap. For eksempel vil en nyansatt få utlevert arbeidsinstrukser for sin nye stilling, men den nødvendige kompetansen opparbeides over tid. Gjennom å utføre oppgavene sammen med andre ansatte som har erfaring vil den nyansatte etterhvert kunne opparbeide seg kompetanse. Læring gjennom aktiv deltakelse gjør at kunnskapen går over til kompetanse,

både for praktisk arbeid men også når det kommer til selskapets kultur og holdninger (Filstad, 2010). Hos oljeselskaper i dag er det vanlig med phishingkampanjer, hvor selskapet selv sender ut phishingmailer som en test for de ansatte. Dette gjør at de ansatte blir bevisste på sin adferd i møtet med mistenkelige e-poster. I tillegg bidrar den aktive deltakelsen til at den enkelte ansatte kan øke sin kompetanse om phishingangrep.

3.2.2 Læring og opplæring

I en digital verden skjer endringer raskt og oljesektoren er intet unntak. Nye teknologiske løsninger og metoder gjør at læring må skje i samme tempo som utviklingen. Et selskaps evne til å utvikle kompetanse og forstå nyskapning blir en viktig faktor for å hindre phishingangrep. Selskaper som ikke har evnen til å omstille seg i takt med de digitale og teknologiske endringene vil kunne ha større vanskeligheter for å hindre phishingangrep. Læring og opplæring er knyttet til informasjon i form av formalisering og dokumenter på den ene siden, men også kunnskap og kompetanse på den andre siden (SINTEF, 2013).

Argote og Ophir (2002) skriver at organisasjonslæring kan ses på som en prosess hvor selskaper gjør endringer som følge av erfaringer de tilegner seg. Man kan lære av både intern og ekstern erfaring. Eksempel på ekstern erfaring er dersom det aktuelle selskapet tar lærdom av cyberangrepet mot Norsk Hydro i mars 2019. Videre definerer Garvin (1993) organisasjonslæring som «*En lærende organisasjon er en organisasjon som er flink til å utvikle og tilegne seg kunnskap, og til å modifisere adferden i forhold til ny kunnskap og innsikt» (s.3).* For et oljeselskap som arbeider med et stort innslag av sikkerhetskritiske aktiviteter vil læring tilknyttet disse aktivitetene være viktig. En kan få læring gjennom en «hindsdight» dimensjon, det vil si at selskapet bruker en tilbakeskuende læring. Eksempelvis gjennom å se hva som gikk galt da en ansatt gikk på et phishingangrep og hvordan de kan hindre at det skjer igjen. På den andre siden kan selskaper bruke «foresight» som en læringsstrategi, dette innebærer å bygge selskapet robust for hendelser som kan skje i fremtiden (Ptil, 2013). Forskjellen ligger i at «hindsight» tar læring av fortiden mens «foresight» forsøker å ta lærdom av hva man tror venter i fremtiden og bygger robusthet ut fra dette.

For et oljeselskap vil det være viktig å hele tiden oppdatere opplæring og oppfølging når det kommer til cybersikkerhet. I en verden hvor teknologien og digitaliseringen utvikles fort vil

det være helt nødvendig for selskapene å følge utviklingen. For at en ansatt skal få informasjon, kunnskap og kompetanse vil et av de viktigste lærepunktene være opplæring (SINTEF, 2013). Ptil sin §22 «*Opplæring i sikkerhet og arbeidsmiljø eller arbeidsmiljøloven*» viser til opplæring i blant annet sikkerhet. I denne paragrafen står det at opplæring er ledere sitt ansvarsområde og det påkreves at arbeidstakere skal få nødvendig opplæring. Samtidig nevnes det eksplisitt at opplæringen skal tilpasses endret risiko og gjentas om nødvendig (Ptil, 2011). For oljeselskapene er opplæring, kunnskap, kompetanse og læring viktige aspekter i kampen mot phishingangrep. Ptil sin §22 viser også til at nødvendig opplæring skal gis og gjennom oppgaven blir det interessant å se i hvilken grad opplæringen er tilfredsstillende nok hos de ulike selskapene. Oljeselskapene som blir undersøkt har store forskjeller både i ressurser og antall ansatte, oppgaven vil forsøke å undersøke om disse faktorene spiller inn på kvaliteten av opplæringen.

3.3 High Reliability Organizations [HRO]

Olje- og gassindustrien er en industri med høy kompleksitet, avansert teknologi og stort risikopotensiale. HRO er organisasjoner som nettopp beskrives som høyteknologiske, til tross for det har de få ulykker og alvorlige hendelser (Engen et al., 2016). I denne oppgaven legges oljeselskapene frem som en HRO-organisasjon, med fokus på kunnskap, kompetanse og kontinuerlig arbeid med sikkerhetskulturen. Disse fokusområdene er viktige i kampen mot phishingangrep.

Teorien om HRO-organisasjoner er basert på studier av organisasjoner som klarer å håndtere kompleks og krevende teknologi uten å bli utsatt for store ulykker. Oljesektoren er som nevnt under kapittel *2.1. Olje og digitalisering* en sektor med høyt fokus på teknologi og digitalisering, likevel setter de alltid sikkerhet høyest. To av suksessfaktorene til en HRO-organisasjon er organisatorisk redundans og evnen til akutte strukturendringer for å kunne tilpasse seg kriser eller plutselige belastningsstopper (SINTEF, 2002). Olje- og gassindustrien blir ofte sett på som en HRO organisasjon. Det forklares ved at de har troen på at ulykker kan forhindres og forebygges ved å hele tiden ha fokus på sikkerhet og pålitelighet. Selskapene som blir brukt i oppgaven er som nevnt forskjellige i størrelse og antall ansatte, noe som kommer tydeligere frem i oppgavens metodekapittel. Videre vil denne forskjellen i størrelse også være interessant å diskutere i lys av et HRO-perspektiv, da ønsket om å operere som en HRO-organisasjon krever både tid og ressurser.

HRO-organisasjoner jobber sammen med tillit, årvåkenhet, kollektiv meningsdanning, kommunikasjon og samarbeid mellom hverandre (Engen et al., 2016). Dette blir gjort gjennom desentralisert styring, god organisasjonskultur og kontinuerlig læring. I en HRO tankegang vil industrien kunne designes som pålitelig. Dette gjøres gjennom fire betingelser:

1. *Sikkerhet og pålitelighet.* Begge deler skal ha høy prioritet i alle ledd av organisasjonen. For oljeselskapene handler det om å hele tiden ha fokus på, og arbeide med sikkerhet. Arbeidet med sikkerhet skal være uavhengig av hvor i organisasjonen du arbeider og hva dine arbeidsoppgaver innebærer (Aven et al., 2018).

2. *Redundans.* Teorien viser til at redundans er med på å øke sikkerheten ved å kompensere for feil. Eksempelvis kan dette omhandle teknologiske løsninger som totrinnsbekreftelse, oppdaterte programvarer og antivirusbeskyttelse. Det er ment som mekanismer som skal fange opp farer og fjerne dem (Aven et al., 2018).

3. *Desentralisert styring, organisasjonskultur og læring.* Gjennom å fordele beslutninger vil beslutningene kunne tas raskere, mer fleksibelt og på lavest mulig nivå. Samtidig setter teorien fokus på en sterk sikkerhetskultur hvor alle oppmuntres til å rapportere inn avvik eller mistanker om feil. Systemene og digitaliseringen utvikler seg, noe som krever at læringen utvikler seg i samme tempo for å kunne opprettholde høyt sikkerhetsnivå (Aven et al., 2018).

4. *Organisatorisk læring*. Viser til i hvilken grad en tar lærdom av andre, tester løsninger og prøver/feiler. Ved å lære av feil kan en rette kurs og unngå lignende hendelser i fremtiden. Eksempelvis har flere oljeselskaper tatt lærdom av selskaper som har opplevd phishingangrep, og fokuset ligger på fordelen av å dele erfaring. En slik læring kan bidra til å redusere antall vellykkede phishingangrep mot oljeselskaper og oljesektoren i sin helhet (Aven et al., 2018).

3.3.1 Sikkerhetskultur og digital sikkerhetskultur

Kultur kan forklares som en gruppe sine holdninger, verdier og sosiale normer (Stranden, 2019). I 1993 begynte det å bli en økende interesse for sammenhengen mellom kultur, sårbarhet og sikkerhet i en organisasjon (Westrum, 1993). I et oljeselskap vil fokuset på sikkerhetskultur være viktig, spesielt for å kunne opprettholde ønsket om å være en HRO-organisasjon. Sikkerhetskultur blir definert som «*atferd knyttet til sikkerhet*» (u.s) og i

organisasjoner handler det om hvilken kunnskap, motivasjon, holdning og adferd de ansatte besitter (NSM, 2014). Ved å kontinuerlig arbeide mot en god sikkerhetskultur kan det bidra til å minske sannsynligheten for at ansatte går på et phishingangrep. Dersom et selskap har en sterk sikkerhetskultur kan en nyansatt enklere be om hjelp dersom de er usikker på om en link er ondsinnet eller ikke. På denne måten vil graden av sikkerhetskultur virke som et tiltak mot phishingangrep. En god sikkerhetskultur vises nemlig i den ansattes atferd (PST, 2015). Sikkerhetskultur kommer som et tillegg til styring av sikkerheten gjennom lover, forskrifter, programmer og prosedyrer. Styrken av sikkerhetskulturen legger føringer for hvilke løsninger og hvor mye ressurser organisasjonen velger å bruke på sikkerheten. Sikkerhetskulturen handler om at en skal forstå hva som er farlig og hvordan en kan bidra til å redusere farene (Aven et al., 2018).

Reason (1997) beskriver sikkerhetskultur som et produkt av de verdiene og holdningene som individer og gruppen besitter. Dette kommer frem i kompetansen og adferdsmønsteret til de ansatte som igjen viser godheten av organisasjonens sikkerhetsprogram. En god sikkerhetskultur er kjennetegnet ved god kommunikasjon, gjensidig tillit, felles oppfatning av sikkerhet og dens betydning samt tiltro til at organisasjonens sikkerhetsmål vil fungere godt (Reason, 1997). Sikkerhetskultur er derimot ikke noe som kommer automatisk, men utviklingen skjer over tid. Norske oljeselskaper og arbeidet med sikkerhet har utviklet seg betraktelig. Etter Alexander L. Kielland ulykken ble Norge ledende på sikkerhet i verden (NOROG, 2017). Videre legger Reason frem fire faktorer som er nødvendig for en god sikkerhetskultur i en organisasjon:

Type kultur	Forklaring
Rettferdig kultur	Handler om hvordan organisasjonen fordeler og behandler skyld og straff. Eksempelvis hvordan de håndterer folk som varsler. I en rettferdig kultur oppmuntres det til å varsle om feil og uriktigheter.
Rapporterende kultur	Henger mye sammen med rettferdig kultur. Den viser til et organisasjonsmiljø hvor rapportering, varsling og bekymringer blir hørt og møtt.
Lærende kultur	Evnen og viljen en organisasjon har til å lære av feil og implementere reformer for å sikre at feil ikke skjer igjen.
Fleksibel kultur	Handler om at organisasjonen klarer å endre og tilpasse seg etter hvilke situasjoner de havner i. Da med hensyn til rapporteringer og beslutninger.

Tabell 2: Fire faktorer for en informert kultur (Reason, 1997).

Disse fire kulturene utgjør tilsammen en informert kultur som er en kultur hvor ledere har kunnskap og kjennskap til menneske, teknologien og organisasjonen (Reason, 1997). Dette er med på å bestemme og lede sikkerheten i et system som en samlet enhet. En god sikkerhetskultur kan bidra til fravær av uønskede hendelser for oljeselskapene. Menneskene som jobber i selskapet blir en del av et fellesskap som sammen har et mål om å drive selskapet på en sikker, strukturert og god måte.

Digital sikkerhetskultur

Oljesektoren er en digitalisert og teknologirettet sektor. Det gir også behov for en sikkerhetskultur med økt fokus på digitalisering. Digital sikkerhetskultur ble i Norge først omtalt av NorSIS i sin rapport «*The Norwegian Cybersecurity culture*» i 2016. En god sikkerhetskultur vil kunne beskytte digitale verdier fra ulike trusler og trusselaktører som angriper systemets innebygde sårbarheter (Bergsjø, 2020). Digital sikkerhetskultur kan videre forstås som våre felles verdier, holdninger, normer, kunnskaper og handlinger i møtet med et økende digitaliserende samfunn. Ved å etablere en god digital sikkerhetskultur kan både den

enkelte og samfunnet i sin helhet bli mer robust mot digitale trusler (NorSIS, 2019). Videre legger NorSIS (2019) frem åtte kjerneområder som er viktige for å bygge en velfungerende digital sikkerhetskultur; adferd, fellesskap, styring og kontroll, tillit, risikoforståelse, vilje til digitalisering, kompetanse og tilslutt interesse. Disse åtte faktorene jobber sammen for å etablere en best mulig sikkerhetskultur. I denne oppgaven er risikoforståelse og kompetanse to spesielt interessante faktorer. Risikoforståelse sier noe om hvorvidt en ansatt kjenner til risiko og konsekvens av et phishingangrep, mens kompetanse er en indikator på hvordan selskapet driver opplæring og oppfølging.

3.3.2 Personellsikkerhet

I denne oppgaven vil det både rettes fokus på nyansatte og etablerte ansatte. Da etablerte ansatte også kan utgjøre en risiko for phishingangrep. NSM (2019) beskriver personellsikkerhet som de tiltak, handlinger og vurderinger som gjøres for å hindre at personell utgjør en sikkerhetsrisiko. For virksomhetene er det viktig å være bevisst på personellsikkerhet både før, under og etter et ansettelsesforhold. Dette innebærer at selskapet blant annet må ha både kompetanse og ressurser samtidig som de ansatte må være klar over hvilke verdier selskapet trenger at de beskytter. I tillegg har selskapet et overordnet ansvar for å etablere en god sikkerhetskultur og øke de ansattes kunnskap og kompetanse når det kommer til sikkerhet og sikkerhetskultur (NSM, 2020).

Personellsikkerhet er relevant for alle organisasjoner med verdier som de ønsker å beskytte (Stranden, 2019). Personellsikkerhet har fokus på forebyggende sikkerhetstiltak med formål å redusere risikoen for uønsket adferd av en ansatt som potensielt kan true sikkerheten. Trening og bevisstgjøring med fokus på sikkerhet er en viktig tilnærming for å kunne etablere en god personellsikkerhet. Trening og bevisstgjøring omhandler blant annet opplæring, kontinuerlig oppdatering av kunnskap samt å motivere ansatte til å arbeide med hensyn til virksomhetens retningslinjer (PST, 2017). I denne oppgaven er trening og bevisstgjøring to viktige faktorer i møtet med et phishingangrep. Kvaliteten av opplæringen og oppfølgingen vil legge føringer for hvor godt egnet de ansatte er i møtet med et phishingangrep.

3.4 Menneske, teknologi og organisasjon

Et oljeselskap er et sosioteknisk komplekst system som består av flere komponenter og mennesker som ledes gjennom et sammenvevd administrativt og organisatorisk system.

Driften i et oljeselskap påvirkers i stor grad av organisatoriske forhold og menneskelige presentasjoner (Bento, 2001). Oljeselskaper må ut fra et helhetlig perspektiv kunne vurdere sårbarhet og risiko som omhandler teknologi, organisasjon og mennesket. NSM (2016) skriver at sårbarheter og tilhørende sikringstiltak kan deles inn i menneskelige, tekniske og organisatoriske. Digitalisering handler ikke bare om teknologi, men også om å kunne designe systemene slik at de begrenser feil. Selskapets sikkerhet kan ikke overlates til den enkelte ansatte. Virksomheten må selv ha tiltak som trer i kraft dersom en ansatt er uheldig å gjør en feil (NSM, 2020). Selv om oljenæringen øker sin automatisering vil det fremdeles være behov for menneske og organisasjon til å etterstrebe krav og overvåke systemene (Ptil, 2019). Mennesket, teknologi og organisasjon er tett bundet sammen i en stadig mer digitalisert oljesektor. I MTO er det samspillet mellom disse tre faktorene som gjør at vi kan sikre oss mot ulykker samtidig som det også kan forårsake ulykker.

Teknologi

For at teknologi skal fungere på best mulig måte må en både kunne styre og bruke den på en riktig måte. Dette gjør at teknologi har begrensninger som også gjør det mulig å utnytte den. Eksempel på utnytting er gjennom et phishingangrep hvor en hacker klarer å lure til seg innloggingsdetaljer til en ansatt. Da unngår hackeren krypteringen og brannmuren som var ment til å hindre slike type angrep (Stranden, 2019).

Organisasjon

Organisasjon er en del som dekker over mye. Blant annet organisering av sikkerhetsressurser, retningslinjer, lagring av informasjon og planer og programmer som har verdi for selskapet. Ofte vil organisasjon være limet mellom teknologien og mennesket, eksempelvis i form av hvilke retningslinjer som legges for databruk og tilgang hos nyansatte i oljeselskapet (Stranden, 2019). I tillegg vil organisasjonens arbeid med sikkerhetskultur legge føringer for hvordan mennesket forstår teknologien samt hvordan teknologien kan tilpasses menneskene.

Mennesket

Mennesker er en sentral del av sikkerhetsarbeidet. Mennesker designer, styrer og vedlikeholder teknologi i alle sektorer, derfor er de også viktige når det kommer til å forårsake og forhindre ulykker (Reason, 1997). Dersom en nyansatt oppdager og rapporterer et forsøk på et phishingangrep har de forhindret en ulykke. Mennesker kan være den eneste grunnen til at vi unngår et phishingangrep i tillegg til å være en faktor som kan utløse et

phishingangrep. Mennesket tar en aktiv del av å trykke på en ondsinnet link, samtidig er det mennesket som kan oppdage angrepet og hindre det fra å eskalere. På tross av dette er det ofte den menneskelige faktoren som får minst oppmerksomhet. En grunn til dette kan være at den menneskelige faktoren er vanskeligere å måle i tall og sette i en kategori (Stranden, 2019).

Mennesket er den mest sårbare faktoren, da mennesker kan feile på flere nivåer og på flere forskjellige måter. Mens teknologi og organisasjon er mer robuste faktorer. Mennesker gjør såkalte latente feil. Latente feil er i følge Reason (1997) feil som er tilstede i et system lenge før man oppdager dem gjennom en uønsket hendelse. Eksempelvis ved at nyansatte ikke har fått god nok opplæring eller etablerte ansatte får for dårlig oppfølging (Stranden, 2019). Sidney Dekker (2006) skiller mellom «The New View» og «The Old View» av menneskelig feil. «The Old View» ser på menneskelige feil som en årsak i seg selv, hvor mennesker er roten til at uønskede hendelser oppstår. Sosiotekniske systemer ville vært trygge hvis det ikke var for menneskelig innblanding. Menneskene som bidrar til uønskede hendelser blir av Dekker omtalt som «Bad Apples». «The New View» har derimot fokus på at ingen mennesker ønsker med vilje å gjøre feil og at feilen derfor må ligge dypere i systemet. En menneskelig feil er bare et symptom på at noe annet er galt lengre bak i selskapet. For eksempel kan det være mangelfull opplæring av nyansatte eller oppfølging av etablerte ansatte. Det er viktig å ikke stoppe opp ved første feil, eksempelvis ved at en nyansatt trykker på en ondsinnet link. Her vil det være avgjørende for videre sikkerhetsarbeid i oljeselskapet å se på bakenforliggende faktorer, som blant annet kan være dårlige teknologiske løsninger, svak opplæring eller manglende kompetanse.

3.5 Oppsummering av teori

Teorier som er lagt frem i dette kapittelet belyser ulike faktorer som kan påvirke hvordan en arbeider for å hindre phishingangrep mot både nyansatte og etablerte ansatte. Det er valgt å fokusere på teorier om risikopersepsjon, som sier noe om ansattes forståelse og kunnskap om risiko og uønskede hendelser. Teorier om kunnskap, kompetanse, læring og opplæring bidrar til å belyse metoder og fremgangsmåter selskapene i oppgaven benytter seg av for å styrke ansatte i møtet med phishingangrep. HRO, sikkerhetskultur og personellsikkerhet legger rammene for hvordan arbeidet med sikkerhet bør foregå i selskapene. Tilslutt sier MTO-teorier noe om forholdet mellom menneske, teknologi og organisasjon i oljesektoren som et sosio-teknisk system.

4.0 Design og metode

I dette kapittelet vil det metodiske grunnlaget for oppgaven bli lagt frem for å best mulig besvare problemstillingen. Gjennom metodedelen skal valgt metode og design forklares og begrunnes. I tillegg vil planleggingen av forskningen og gjennomføringen bli tydelig beskrevet før kvalitetskriteriene validitet, reliabilitet og overførbarhet blir diskutert. Tilslutt i kapittelet vil styrker og svakheter ved anvendt metode bli diskutert.

4.1 Metodisk tilnærming

4.1.1 Forskningdesign

Bakgrunnen for studiet var ønsket om å lære mer om cyber security og hvilke type digitale trusler og sårbarheter som finnes i oljesektoren. Dette dannet videre grunnlaget for problemstilling og etterhvert tilhørende forskningsspørsmål. Oppgavens problemstilling ble tilslutt:

I hvilken grad utgjør nyansatte en større risiko for phishingangrep enn etablerte ansatte i oljesektoren?

Underveis i prosessen har både problemstilling og forskningsspørsmål blitt endret og justert. Problemstilling og forskningsspørsmål er det viktigste elementet av ethvert forskningsdesign. Det er forskningsspørsmålene som vil avgjøre hvilket design som er hensiktsmessig å bruke for å komme frem til et best mulig svar (Blaikie, 2019). I følge Blaikie (2019) er et forskningsdesign noe som skal være forberedt av forskeren før prosjektet med innsamling av data blir igangsatt. Forskningsdesignet blir brukt som en guide eller en plan for selve forskningsprosjektet (Blaikie, 2019). I undersøkelsen av problemstillingen er det lagt til grunne ulike forskningsspørsmål for å bedre kunne forstå hvordan oljeselskaper arbeider for å hindre phishingangrep. Formuleringen av forskningsspørsmålene er derfor det virkelige startskuddet for forberedelsene av et forskningsdesign. Denne oppgaven går ut på å forstå i hvilken grad nyansatte utgjør en større risiko for phishingangrep enn etablerte ansatte i oljesektoren. Oppgavens generelle forskning vil ta utgangspunkt i å utforske, beskrive, forklare og forstå faktorer som kan bidra til dette.

I oppgaven vil jeg benytte meg av abduktiv forskningsstrategi. Formålet med denne strategien

er å beskrive og forstå sosiale liv når det gjelder sosiale aktørers mening og motiv fra innsiden. Som forsker skal jeg ikke ta på meg rollen som utenforstående aktør og vurdere verden fra dette ståstedet, den sosiale forskerens oppgave er å oppdage og beskrive informantens syn og ikke sitt eget. Derfor er målet å oppdage hvorfor ansatte og oljeselskaper gjør det de gjør ved å avdekke gjensidig kjennskap, de symbolske betydninger, intensjoner og regler som gir retninger for deres handlinger (Blaikie, 2019). I følge Danermark (2002) er en styrke ved abduktiv forskningsdesign at den gir veiledning for tolkningsprosessen som vi tilskriver mening til hendelser i forhold til en større sammenheng. I abduksjon vil jeg relatere teori til observasjon, for deretter å trekke rimelige antakelser som er i tråd med den valgte teorien.

4.1.2 Kvalitativ forskningsmetode

Innenfor forskningsmetoden skiller man gjerne mellom kvalitativ og kvantitativ metode. Forskjellen ligger i hvordan man innhenter og analyserer data. Kvantitative metoder er generelt opptatt av å telle og måle aspekter ved det sosiale liv, mens kvalitative metoder er mer opptatt av å produsere diskursive beskrivelser og utforske sosiale aktørers meninger og tolkninger (Blaikie, 2019). Det er vanlig å bevege seg i én av retningene. For å svare på oppgavens problemstilling vil jeg benytte meg av kvalitativ metode for å kunne avdekke flere sider ved temaet. Samtidig kan jeg ved hjelp av denne metoden innhente en bedre forståelse av forhold som kan være med på å forklare viktigheten av arbeidet med å forhindre phishingangrep (Holme & Krohn, 1998). Kvalitativ metoder som blir brukt i denne oppgaven er dokumentanalyse og intervjuer. Til sammenligning vil det i kvantitative studier brukes tall for å generere statistikk. Aase og Fossåskaret (2014) forklarer at kvalitative metoder går i dybden, mens de kvantitative søker mer i bredden. På bakgrunn av dette kan en si at dokumentanalyse og intervjuer som metoder gir meg en dypere forståelse om de faktiske forholdene jeg undersøker.

Siden studiet har et eksplorativt design, med gjentakende endring av både problemstilling og forskningsspørsmål underveis i undersøkelsen av fenomenet, ville ikke en kvantitativ tilnærming fungert. Ved å bruke kvalitativ metode får jeg et grunnlag til å fordype meg i det fenomenet som jeg studerer (Aase og Fossåskaret, 2014). For å oppnå best mulig kunnskap og forståelse om hvordan oljeselskaper arbeider for å hindre phishingangrep fant jeg det derfor hensiktsmessig å bruke kvalitativ forskningsmetode.

4.2 Forskningsprosess

Tabellen under gir en oversikt over forskningsprosessen jeg har vært gjennom i etableringen av denne oppgaven. Den viser i tillegg formål og utfall av de ulike aktivitetene forbundet med prosessen. Arbeidet har vært preget av kontinuerlige endringer og omjusteringer, selv om tabellen fremstilles som ryddig med klare skiller vil jeg påpeke at det ikke har vært slik i praksis, noe som er i tråd med et eksplorativt design.

Når	Aktivitet	Formål	Utfall
Januar	Etablerte en skisse med innledning og kontekst. I tillegg til gjennomgang av aktuell litteratur og utarbeiding av problemstilling og forskningsspørsmål.	Komme tidlig i gang med skisse for å skrive ut ideer og tanker. Opparbeide meg kunnskap om tema og hvilken forskning som har blitt gjort rundt phishingangrep.	Fikk en bedre forståelse for tema. Synes temaet virket veldig interessant og fikk kunnskap som jeg kunne bruke gjennom hele prosjektet.
Februar	Utvikling av forskningsdesign, teori og intervjuguide.	Forsøke å stake ut en retning og skape en ramme som grunnlag for empirisk undersøkelse. Ved å utarbeide en teoretisk forståelse vil det bidra til kunnskap for å stille de riktige spørsmålene i intervjuguiden.	Den teoretiske tilnærmingen ble delvis etablert, forskningsdesign ble skissert og intervjuguiden ble utformet. Aktuelle intervjuobjekter ble identifisert.
Mars	Fortsatte skriving av kontekst, teori, metodekapittel og arbeidet med	Ønsket å begynne på datainnsamlingen og skrive mer utfyllende på metoden.	Innledning og kontekst ble ferdigstilt. Intervjuet bidro til endring av

	problemstilling og forskningsspørsmål. Tok kontakt med fire intervjuobjekter i uke 12, fikk et avslag og to svar. Gjennomførte et intervju ganske umiddelbart. Transkriberte intervjuet og gjorde forbedringer i intervjuguiden. I slutten av mars tok jeg kontakt med to nye selskaper i håp om å få flere intervjuer.	Intervjuene ble gjort for å gi data til oppgaven og videre grunnlag til å skrive mer på metodedelen samt finjustere intervjuguiden. Funn fra det første intervjuet bidro også til en endring i problemstillingen.	ordlyd i problemstillingen og noen små endringer i teorien. Intervjuguide ble også formulert litt annerledes etter endring av problemstilling. Transkriberingen bidro til å bekrefte mine antakelser samtidig som det ga mulighet til å begynne på empirikapittelet.
April	De to første dagene i april fikk jeg gjennomført to intervjuer. Samtidig kontaktet jeg fem nye selskaper for å få intervjuer. Skrev metodekapittel med utgangspunkt i de tre intervjuene jeg til nå hadde gjort. Begynte å samle og strukturere intervjuene for empirikapittelet.	Samle inn mer empiri. Ønsket å få mer datagrunnlag. Samtidig var jeg klar for å begynne på diskusjonen og ønsket å få samlet dataen jeg allerede hadde til et empirikapittel. Stikkordene jeg skrev i empiri og diskusjon gjorde det enklere å få oversikt	Lyktes ikke med å få flere intervjuer. Tenkte at dersom jeg fikk flere informanter måtte jeg bare flette dem inn i empirien underveis. Metodekapittelet ble så og si ferdigskrevet. Empirikapittelet ble utskrevet i slutten av april.

	Skrev i stikkordsform hva som skulle med i både empiri og diskusjonskapittelet.	samt å skrive ut stoffet.	
Mai	Begynte å skrive på diskusjonen. Skrev så ut konklusjon og videre forskning. Tok deretter en ny gjennomgang av diskusjonen for å supplementære. Gjorde endringer på et forskningsspørsmål. Som følge av endringen av forskningsspørsmålet ble det også gjort små endringer i teori- og metodekapittelet.	Ønsket å begynne å ferdigstille oppgaven og samle en rød tråd. Endringen av et forskningsspørsmål ble gjort for å kunne gi oppgaven mer data i form av dokumentstudier. Endringene i teori- og metodekapittelet ble gjort for å binde forskningsspørsmålet bedre sammen med resten av oppgaven.	Oppgaven begynte å ta form. Endring av forskningsspørsmål ga et positivt utfall med mulighet for mer diskusjon i oppgaven. Teori- og metodekapittelet ble mer sammenhengende med resten av oppgaven.
Juni	Leste korrektur av oppgaven og gjorde små endringer etter siste veiledning. Gjennomgikk alle referanser og la inn korrekt sidetall og tabeller.	Få vekk skrivefeil, referansefeil og selvfølgeligheter i tillegg til å samle en rød tråd. Omstrukturerte diskusjonen for å unngå gjentakelse.	Oppgaven ble ferdigstilt og levert 12.06.2020.

Tabell 3: Forskningsprosess (Eget arbeid, 2020).

4.3 Datainnsamling

Kvalitativ metode åpner opp for å gjennomføre intervjuer og studere dokumenter. Som følge av Corona var jeg nødt til å gjøre endringer i datainnsamlingen. I første omgang ønsket jeg at datainnsamlingen i all hovedsak skulle komme fra intervjuer. Da dette ikke lot seg gjøre startet jeg arbeidet med å lete etter relevante dokumenter som kunne bidra til å belyse mine forskningsspørsmål med tilhørende problemstilling.

4.3.1 Dokumentstudie

Dokumentstudiet har blitt grunnlagt gjennom ulike dokumenter som offentlige utredninger, nasjonale trusselvurderinger, NOUer, nyhetsartikler, temarapporter, rapporter om risiko og sårbarhet i oljesektoren samt dokumenter fra relevante aktører. I dokumentene har jeg forsøkt å finne relevant stoff om både cyberangrep, IKT-sikkerhet, phishing og de ansattes rolle og tilnærming til cyberrisikoer. Det finnes utrolig mye stoff som omhandler cyberangrep, IKT-sikkerhet og phishingangrep. I tillegg finnes det noen rapporter som i enkelte deler av rapporten tar for seg phishingangrep mot oljesektoren. Videre har det vært få dokumenter som eksplisitt har omhandlet nyansatte og vurdering av deres risiko og sårbarhet i møtet med et phishingangrep. På bakgrunn av Corona ble det utfordrende å få intervjuer med informanter, derfor ble dokumentstudiet enda viktigere.

Sommeren 2014 ble flere norske oljeselskap utsatt for et stort phishingangrep. Angrepet bidro til å sette phishing og datasikkerhet på dagsorden. På bakgrunn av dette valgte jeg å bruke blant annet PST sine trusselvurderinger og NSM sine sårbarhet- og risikovurderinger fra de siste fem årene som datagrunnlag for oppgaven. Det vil si fra 2015 til 2020. Både PST og NSM kommer årlig ut med vurderinger av ulike trusler, risikoer og sårbarheter som kan komme til å ramme Norge i det kommende året. Vurderingene fra PST og NSM ble gjennomgått for å kartlegge informasjon om datasikkerhet og phishingangrep som kan være relevant for oppgaven. Dette ble gjort for å kunne undersøke i hvilken grad PST og NSM har fokusert på phishingangrep som en del av det nasjonale sikkerhetsbildet.

4.3.2 Definere utvalg

Nøkkelinformanter er personer som en anser å ha spesielt god oversikt over og innsikt i temaet som skal belyses (Andersen, 2006). Som nevnt tidligere gjorde Coronaviruset det

vanskelig å få tak i informanter. Derimot var de informantene jeg fikk intervjue i besittelse av mye og god informasjon rundt temaet cyber security og phishingangrep. Nøkkelinformanter er interessante informanter nettopp fordi de er ressurssterke personer som gjennom sin erfaring og posisjon kan belyse en sak eller et fenomen. Deres informasjon og kunnskap er viktige for meg som forsker. Nøkkelinformantene sin beskrivelse av sine subjektive opplevelser gir et viktig grunnlag for meg som forsker til å forstå, analysere og legge frem de aktuelle hendelsene og prosessene (Andersen, 2006). Helst ønsket jeg å bruke personer som hadde jobbet i selskapet en stund og som var kjent med opplæring- og oppfølgingsrutiner når det kom til IKT-sikkerhet hos ansatte. I denne oppgaven har jeg valgt ut informanter fra forskjellige oljeselskaper som nettopp innehar denne kompetansen.

Tilsammen i oppgaven blir det brukt tre forskjellige informanter, alle jobber i ulike selskap med stor spredning i antall ansatte, omfang og ressurser. Dette ble som nevnt i teorien gjort for å bedre kunne belyse og sammenligne hvordan små og store oljeselskaper jobber med phishing som trussel. I og med at spekteret i selskapene går fra noen hundre ansatte til flere titall tusen ansatte ønsket jeg å undersøke forskjellige arbeidsmetoder for integrering av nyansatte med fokus på cyber security og spesielt phishing. I oppgaven har jeg valgt å holde nøkkelinformantene og selskapene anonyme. Dermed blir verken oljeselskap eller informantene navngitt. Dette fordi jeg ikke ser det som avgjørende eller relevant for oppgaven at dette blir utelatt. Informantene vil i empiri og drøfting bli omtalt som:

Informant	Stillingstittel	Stillingsbeskrivelse	Selskap
Informant 1 (IN1 i teksten)	Senior Security Professional	Informantens arbeidsoppgaver innebærer å vurdere ulike risikoer. Eksempelvis sikringsrisikoer som kan oppstå i forhold til virksomheten, fysisk, personell og informasjonssikring. Følge opp og implementere tiltak i	**Selskap Medium (Selskap M i teksten)** Selskapet er det mellomste selskapet i størrelse. Videre har de kontorer flere steder i Norge, i tillegg til hovedkontoret. Selskapet er det nest

		den forbindelse.	største av de tre selskapene som blir brukt i denne oppgaven.
Informant 2 (IN2 i teksten)	Senior IS Business Analyst	Informanten jobber i IT-avdelingen med forskjellige IT-prosjekter som en link mellom business og IT. Har hovedansvar for leting, drilling og boring.	**Selskap Small (Selskap S i teksten)** Selskapet er det minste selskapet som blir brukt i oppgaven. Hovedkontoret ligger i et annet land enn Norge. Dermed er dette selskapet det minste selskapet som blir brukt i denne oppgaven.
Informant 3 (IN3 i teksten)	IT-manager	Arbeidsoppgavene går ut på at informanten skal ha oversikt over at forretningsområdet følger de retningslinjene som er gitt av selskapet. I tillegg har informanten en rolle som går på IT-sikring.	**Selskap Large (Selskap L i teksten)** Selskapet er det største som blir brukt i oppgaven. Noe som gjør selskapet til det største i denne oppgaven. Hovedkontoret ligger i Norge.

Tabell 4: Informanter (Eget arbeid, 2020).

4.3.3 Intervju og intervjusituasjon

I kvalitative studier ønsker forskeren å forstå kompleksiteten av feltet som studeres. Studiene ble skapt ut fra ønsket om å forstå «den andre» (Postholm, 2004). Fra min side var det viktig å få problemstillingen belyst ved hjelp av aktørenes egne erfaringer med phishingangrep i oljesektoren. Gjennom å bruke intervju som datainnsamlingsmetode kan jeg undersøke om det er samsvar mellom normative premisser og praksis, eller om det er avvikende. Samtalebasert intervju kan ofte være ustrukturerte, usystematiske, åpne, tematiske eller kvalitative (Andersen, 2006). Slike intervjuer er veldig forskjellige fra kvantitative intervjuer hvor struktur og dynamikk ikke preger samtalen. For denne oppgaven vil samtalebaserte intervjuer være hensiktsmessig, da formålet er å ha en passiv lyttende rolle med åpne spørsmål hvor informantens svar vil styre og prege settingen.

I lys av Coronapandemien har det ikke vært enkelt å få tak i informanter som jobber med cyber security i oljesektoren. Jeg kontaktet i første omgang fire stykker i midten av mars. To var tilgjengelig for intervju, en ga avslag og den siste svarte ikke. Dermed bestemte jeg meg for å sende intervjuforespørsel til to nye oljeselskap. En godtok og en svarte ikke. I et siste forsøk kontaktet jeg fem oljeselskaper til, men heller ikke her lykkes jeg i å få intervjuer. På bakgrunn av dette endret jeg forskningsspørsmål nummer en for å bedre kunne fylle ut og supplementære datagrunnlaget med dokumentstudier.

Intervjusituasjonene var alle veldig forskjellige. Intervjuet med informant 1 var preget av at informanten ikke hadde kapasitet til å ta intervjuet på datoene som først ble foreslått, dette gjorde at vi måtte ta intervjuet så raskt som mulig. Som følge av Corona ble intervjuet tatt over Skype og samtalen ble tatt opp. Intervjuguiden ble forsøkt ferdigstilt og jeg fant ut at intervjuet bare måtte gjennomføres så kunne intervjuguiden bli optimalisert i etterkant. Intervju med informant 2 ble tatt over telefon, dermed mistet jeg muligheten til å ta opptak av samtalen. Intervjuet med informant 3 ble gjort over Skype og jeg hadde mulighet til å ta opptak av samtalen. På grunn av situasjonen med Corona ga jeg informantene mulighetene til å gjennomføre et kortere intervju enn først planlagt. I utgangspunktet ønsket jeg intervjuer på 45-60 minutter men ga beskjed om at intervjuene kunne kortes ned dersom de hadde behov for det. Dette ble gjort for å vise forståelse for at vi er i en vanskelig situasjon og jeg kunne ikke be om alt for mye tid fra dem. Ikke bare gjorde Coronaviruset at flere måtte jobbe

hjemmefra med begrensede midler, men det ga også økt risiko for cyberangrep. Mine informanter jobbet alle med IT og cybersikring og var naturlig nok svært travle i denne perioden.

4.3.4 Intervjuguide

Ofte har dataen som blir samlet inn gjennom ustrukturerte intervjuer en tendens til å gå på sammenligning av mennesker (Wadel, 2014). I dette tilfellet vil det være naturlig å sammenligne de ulike informantenes svar og bilde av situasjonen. Jeg fokuserer på deres spesifikke beskrivelser av phishingangrep som en trussel mot oljesektoren. I forkant av intervjuene har jeg lest meg godt opp på teorien og fagstoffet som er relevant for oppgaven. I tillegg har jeg kjennskap til oljesektoren fra et tidligere arbeidsforhold. Betydningen av forkunnskap før et intervju kan diskuteres. Noen mener det er en fordel å vite så lite som mulig om det aktuelle temaet, for å ikke påvirkes av forutinntatthet. På den andre siden kan forskere uten forkunnskap misforstå og misoppfatte budskapet til informanten. Det er derimot viktig for meg som forsker å ha tilstrekkelig forståelse for rammene for samtalene og de sosiale interaksjonene jeg inngår i (Andersen, 2006).

Intervjuguiden ble utformet i forkant av intervjurundene. Et viktig punkt er at spørsmålene ble formulert på en slik måte at informantene må tenke og reflektere over spørsmålet. Dette mener jeg gir mer utfyllende svar enn å kun stille «ja» eller «nei» spørsmål. Etter første intervju gjorde jeg endringer i ordlyden på problemstillingen, dette bidro også til endringer i selve intervjuguiden. Overflødige spørsmål ble luket vekk og spørsmålene ble delvis endret for å bedre kunne belyse problemstilling og forskningsspørsmål. Spørsmålene ble delt opp etter hovedtema, men jeg ønsket fremdeles å ha et fleksibelt forhold til spørsmålene. Dersom en informant svarer veldig utfyllende på et spørsmål vil det ikke være nødvendig å stille et lignende spørsmål senere i intervjuet. Som forsker var jeg lyttende samtidig som jeg ønsket å være i stand til å ta initiativ uten å lede svaret i en bestemt retning (Andersen, 2006). Dette mener jeg bidro til en bedre flyt i intervjuet, samtidig som informanten fikk snakke fritt. Intervjuet bar preg av at jeg som forsker var fleksibel til å gjøre endringer underveis, da både i rekkefølgen og formuleringen av spørsmålene. Dette ble gjort for å lettere kunne følge opp de svarene som blir gitt og informasjonen informantene la frem (Thagaard, 2013).

4.3.5 Forsker- og informantforholdet

Informantintervjuing er en bestemt form for sosial samhandling. Slike samtaler er uten unntak preget av spenninger og motsetning knyttet til de ulike rollene som forsker og informant. Intervjuet kan få innslag av sosial intimitet, men skal likevel ikke bli for personlig. Selv om intervjusituasjonen er en sosial situasjon, skal den forholdes profesjonell (Andersen, 2006). For meg var det viktig å være ærlig på at jeg var en student, og dermed ikke hadde komplett oversikt over oljenæringen og dens cybertrusler. Likevel var jeg godt forberedt til intervjuene i form av å lese meg opp på dokumenter og publikasjoner. Som nevnt i *4.3.4 Intervju og intervjuguide* har jeg tidligere jobbet i oljesektoren, dermed hang jeg godt med i samtalen og opplevde i liten grad at jeg måtte spørre om forklaring av informantenes svar.

Istedenfor å betrakte strukturering av intervjuguiden som enten/eller valgte jeg å semi-strukturere intervjuene for å gi mer rom for fleksibilitet. Målet var at jeg ikke skulle overstyre eller lede svar i en bestemt retning (Andersen, 2006). Med dette ønsket jeg at informanten skal kunne komme med tilleggsinformasjon og avdekke interessante aspekter ved det aktuelle intervjuspørsmålet. Semi-strukturering innebar en intervjuguide som var fastsatt på forhånd med tema og spørsmål i fast rekkefølge. Noen spørsmål med ja/nei-svar fikk oppfølgingsspørsmål som «hvis ja – hvorfor?». Dette gjorde jeg for å sikre at temaene jeg ønsket å få belyst ble besvart av informantene. I tillegg ble alle informantene gjort oppmerksom på at intervjuguiden ble skrevet før coronaviruset nådde Norge, dermed skulle de besvare spørsmålene uten å ta hensyn til situasjonen coronaviruset nå har satt oss i. Dette innebar at informantene skulle besvare spørsmålene ut fra hvordan hverdagen så ut før Corona.

4.4 Kvalitetskriterier

I dette delkapittelet vil jeg drøfte oppgavens reliabilitet, validitet og overførbarhet. Samt argumentere for valgene mine underveis i forskningen. Tilslutt tar jeg opp etiske problemstillinger og hvordan jeg som forsker må forholde meg til disse gjennom hele oppgaven.

4.4.1 Reliabilitet og validitet

Reliabilitet og validitet er to gode kriterier når det kommer til kvaliteten på kvalitativ forskning. Reliabilitet kan forstås som pålitelighet mens validitet viser til dataens gyldighet

(Tjora, 2012). Videre forklarer Tjora (2012) at gyldigheten til forskeren forsterkes gjennom å være åpen i hvordan forskningen blir praktisert. Dersom forskningen blir gjort i henhold til faglige rammer og er fastholdt i annen relevant forskning vil dette høyne gyldigheten til studiet.

Reliabilitet

Reliabiliteten blir ifølge Holme & Solvang (1996) bestemt ut fra hvordan målingene er gjort. Reliabiliteten til dataen avgjøres dermed av hvor pålitelige dataene er. Det finnes to måter å måle reliabilitet på. Den første er «test-retest-reliabilitet», det går ut på at samme informanter skal bli undersøkt på nytt kun noen uker etter første undersøkelse. Dersom resultatene blir de samme som sist har studiet høy reliabilitet. Den andre måten kalles «interreliabilitet», her skal flere forskere undersøke samme fenomen og komme frem til det samme resultatet. Reliabilitet knyttes til nøyaktigheten av dataen, hvordan den brukes, samles inn og bearbeides (Johannessen et al, 2010). Et godt argument for reliabiliteten i denne oppgaven vil være at jeg har brukt tilnærmet lik intervjuguide gjennom alle intervjuene og informantene har blitt stilt omtrent de samme spørsmålene. Dermed kan etterprøvbarheten av forskningen min være lettere å bevise. Informantene mine var kompetanserike og som forsker i møte med dem ønsket jeg å være bevisst og aktiv. Dette gjorde jeg som nevnt i *4.3.5 Forsker- og intervjuforholdet* ved å lese meg godt opp på fagstoffet i forkant av intervjuet. Denne aktive forskerrollen bidro til å gi en større uttelling i form av analytisk kontroll, noe som bidrar til økt validitet og reliabilitet (Andersen, 2006). Videre skriver Tjora (2012) at personlig interessere og engasjement kan påvirke forskningen både positivt og negativt. Oljesektoren er som nevnt i *4.3.4 Intervju og intervjuguide* en sektor jeg har jobbet i, samtidig har jeg en stor interesse for cyber security og de utfordringer det fører med seg. Gjennom forskningsprosessen har jeg vært bevisst på kjennskapet til sektoren og brukt engasjementet mitt som en fordel. Dermed vil jeg si at min personlige interesse ikke har hatt særlig negative effekter på oppgaven.

Ifølge Repstad (1993) kan stedsvalg påvirke utfallet av intervjuet og at det derfor er viktig og velge en plass hvor informanten kan føle seg komfortabel (Tjora, 2012). Som forsker ønsket jeg å ta intervjuene på informantenes arbeidsplass, dette hadde optimalt sett vært det beste. Grunnet spredningen av Coronaviruset lot ikke dette seg gjennomføre. Intervjuene måtte ta plass over Skype og vanlig telefonsamtale, dette kan påvirke reliabiliteten. Jeg ga alle informantene muligheten til å velge hvilken kommunikasjonsmetode de ønsket å bruke, men

presiserte at Skype var ønskelig. To intervjuer ble gjort over Skype mens et ble gjort over telefon, noe som også var fordelaktig da jeg ikke bor i samme by som informantene. Ifølge Jacobsen (2010) vil bruk av telefon- og videosamtaler redusere kostnad i tillegg til å spare tid. Samtidig poengteres det at personer oftere har lettere for å snakke om følsomme tema ansikt til ansikt. Ved to av intervjuene hadde jeg muligheten til å se informantene via videokamera, på denne måten kunne jeg delvis lese kroppsspråket. I telefonintervjuet fikk jeg som forsker ikke muligheten til å observere informanten. Jeg hadde da ikke muligheten til å lese kroppsspråk og faren kunne være større for at jeg «trår over en grense» (Jacobsen, 2010). Derimot opplevde jeg ikke dette i noen grad hverken i telefonsamtalen eller ved intervjuene over Skype.

Validitet

Dersom et datasett har høy validitet vil det si at man har klart å finne utav det man i starten av forskningen satte seg som mål. I tillegg til at dataene en har funnet er gode og troverdige (Holme og Solvang, 1996). Intervjuene jeg har gjennomført ble gjort med tre personer fra forskjellige oljeselskaper. Dermed kan jeg ikke påstå at svarene mine er generaliserbare. Med dette menes at svarene ikke gjenspeiler alle oljeselskap i Norge. For å få til dette måtte jeg har intervjuet informanter fra alle oljeselskaper i Norge, noe som hadde vært svært vanskelig med tanke på tid og ressurser. I all hovedsak dreier validitet seg om det er samsvar mellom fenomenet som skal undersøkes og resultatene en kommer frem til (Johannessen et al., 2010). I tillegg har nøkkelinformantene fått valget om å se over utkast for å komme med innspill eller rammer, dette ble gjort for å skape et godt utgangspunkt for empiri og diskusjonen videre i oppgaven (Yin, 2014).

For videre å øke validiteten har det blitt brukt dokumentstudier som omhandler datasikkerhet og phishingangrep. Dokumentene har inneholdt både generelle vurderinger men også vurderinger spesifikk rettet mot oljesektoren. I dokumentstudiet har jeg hovedsakelig gjennomgått tidligere forskning, NOUer og veiledere gitt ut av både PST og NSM. Dette har blitt gjort for å gi oppgaven tyngde og gode bidrag til empirien.

4.4.2 Etiske problemstillinger

I vitenskapelig praksis er en underlagt noen forskningsetiske retningslinjer som både omhandler uformelle og formelle lover. Disse er laget for å beskytte deltakerne i ulike forskningsprosjekt. På bakgrunn av dette må jeg som forsker være presis og sann i hele

prosjektet. I tillegg er jeg underlagt og må ta hensyn til personopplysningens krav, som innebærer anonymisering, tilstrekkelig informasjon og pålitelighet (Thagaard, 2013). Dette ble gjort ved å holde informantene anonyme og i tillegg oppfordre dem til å ikke nevne navn eller selskap i intervjuet, da det ble tatt opptak av intervju. I forkant av intervjuet ga jeg også beskjed til informantene om at jeg ville sende dem en samtykkeerklæring på mail. På grunn av coronaviruset og det faktum at informantene hadde hjemmekontor ble samtykkeskjemaet godkjent ved å skrive «*Jeg godtar samtykkeerklæring*» på e-post til meg.

4.5 Styrker og svakheter ved metode

Ved å ta i bruk kvalitativ metode med semi-strukturert intervju ga jeg informantene få begrensninger i hvordan de ønsket å besvare spørsmålene. Opptak av intervju gjorde også at jeg kunne la informantene snakke fritt uten å måtte stoppe dem for å få tid til å notere ned hva de sa. I telefonintervjuet skrev jeg samtalen ned i stikkordsform konstant gjennom hele intervjuet. Selv om jeg hadde lagt opp en intervjuguide med klare spørsmål og tema lot jeg samtalen flyte fritt, noe som er en styrke for datainnsamlingen. Dokumentstudiet har også bidratt til å styrke oppgaven. Dokumentene som ble undersøkt har gitt meg god bakgrunnsinformasjon til bruk i intervjuguiden men også til å skrive ut empirien. I tillegg hadde jeg kunnskap og erfaring fra oljesektoren, noe som gjorde at jeg hang med i samtalen også når informantene brukte typiske forkortelser og faguttrykk fra oljesektoren. Erfaringen gjorde at jeg unngikk å stanse samtalen for å få oppklaring i ord og uttrykk. Dette gjorde at samtalen fikk en naturlig flyt uten for mange pauser til oppklaring av faguttrykk.

Videre valgte jeg å anonymisere både informant og selskapet de jobbet i. Cyber security og sårbarheter forbundet med ansettelsesforhold i oljesektoren kan være et sensitivt tema, spesielt når jeg ber dem fortelle om cyberangrep selskapet selv har opplevd. Formålet med å holde alt anonymt var at informantene skulle være trygge på at informasjonen de kom med ikke kunne spores tilbake til dem eller selskapet de jobbet i. På denne måten gir det rom for informantene til å komme med mer detaljerte og interessante forklaringer på hvordan deres selskap jobber med phishing som trussel, og da spesielt i en ansettelsesprosess. Valget om å anonymisere informantene og deres selskap ser jeg på som en stor styrke for oppgaven. Ved å være anonyme fikk jeg inntrykk av at informantene forklarte dypere hvordan de jobber med cyber security men også hvilke sårbarheter selskapet har i møte med kriminelle aktører.

Ulempene ved kvalitativ metode fikk jeg også oppleve. Informantene jeg ønsket å bruke til

oppgaven var som nevnt personer som jobbet med cyber security i oljesektoren. Gjennom min erfaring i oljesektoren har jeg bekjente som jeg benyttet meg av for å få informanter. Det viste seg å være vanskeligere en først antatt å komme i dialog med personer jeg ønsket å ha som informanter. Gjennom mine bekjentskap ble jeg sendt videre til personer som vedkommende mente ville være gode informanter til min oppgave. Dessverre stoppet kontakten der, selv etter gjentatte purringer. På grunn av coronaviruset og det faktum at oljeprisen sank var det et uheldig tidspunkt å forsøke å få tak i informanter i oljesektoren på. Samtidig ble cybertrusselen høynet som følge av at flere og flere måtte ha hjemmekontor for å redusere smittefaren av coronaviruset. Dette gjorde naturlig nok at personer som jobber med cyber security i oljesektoren var svært opptatte. Jeg kontaktet tilsammen 11 oljeselskaper men fikk kun tre intervju. Datagrunnlaget for oppgaven ble derfor mye smalere enn ønsket, noe som er en klar svakhet.

Intervjuene som ble gjort ble gjennomført på telefon og Skype. Grunnet coronaviruset og situasjonen vi var i med tanke på smittevern ville det uansett vært uaktuelt å møte informantene for et intervju ansikt til ansikt. Intervju på kontoret til informantene eller annen ønsket lokasjon ville selvfølgelig vært det mest optimale, men dette lot seg ikke gjøre og kan ses på som en svakhet. I dialogen med informantene i forkant av intervjuene ga jeg beskjed om at intervjuene kunne kortes ned. I tillegg sa jeg i begynnelsen av selve intervjuet at jeg skulle holde det kort og presist slik at jeg ikke tok opp for mye av deres tid. Dette virket å fungere godt, og for å sikre meg at informantene fikk sagt det de ønsket avsluttet jeg hvert intervju med spørsmål om de ønsket å legge til noe. Til slutt fikk jeg også godkjennelse av alle til å sende oppfølgingsspørsmål på mail dersom jeg hadde behov for det. At intervjuene måtte kortes ned kan være en svakhet, likevel føler jeg at informasjonen som ble gitt fra informantene i intervjuet dekket forskningsspørsmålene mine. Og dermed er tilstrekkelig god nok til å kunne fungere som datagrunnlag for oppgaven.

5.0 Empiri

I empirikapittelet vil resultatene fra innsamlet datamateriale bli presentert. Dataen består av dokumentstudier og tre informantintervjuer. Målet er at de empiriske funnene skal legges frem for å bedre kunne bruke innsamlet informasjon til tolkning og diskusjon av problemstilling og forskningsspørsmål i delkapittel 6. Empirikapittelet er sortert etter forskningsspørsmålene, dermed vil det i kapittel 5.1 presenteres hvordan oljesektoren har erkjent og forholdt seg til phishing og hvordan de fokuserer på nyansatte i møtet med phishingangrep. 5.2 redegjør for rollen kunnskap og kompetanse spiller i møtet med phishingangrep mens 5.3 viser til hvordan oljeselskapene jobber for å hindre phishingangrep.

5.1 Hvordan har oljesektoren erkjent og forholdt seg til phishing som en cybertrussel, og i hvilken grad har en fokusert på nyansatte som en sårbar gruppe i forhold til denne trusselen?

5.1.1 Cybertrusler i oljesektoren

PST kommer årlig ut med en trusselvurdering for Norge. I 2015 var hovedfokuset i trusselvurderingen på ekstremisme og politisk motivert vold. Likevel nevnes dataangrep som en mulig sårbarhet Norge må ta høyde for i 2015. PST (2015) skriver videre at petroleumssektoren kan være et mulig offer for en slik handling. I trusselvurderingen gjort for 2016 er dataangrep fremdeles ikke et av de største fokusområdene for PST (PST, 2016). Det nevnes kun at dataangrep kan være et mulig virkemiddel for ondsinnede aktører. PST sin trusselvurdering for 2017 har derimot dataangrep som et hovedpunkt. Det utdypes at Norge og norske interesser er attraktive mål for fremmed etterretningsvirksomhet (PST, 2017). I trusselvurderingen for både 2018 og 2019 skriver PST at de regner med at Norske virksomheter vil bli utsatt for nettverksangrep (PST, 2018; PST, 2019). Dette blir videre nevnt som tydelige trusler for Norge også i trusselvurderingen for 2020 (PST, 2020).

NSM utgir også årlig en risikovurdering for hvilke risikoer Norge vil stå ovenfor i det kommende året. I NSM sin risikovurdering for 2015 konstaterer de at risikoen for flere dataangrep er høy. Dette kommer også frem i risikovurderingene for 2016, 2017, 2018, 2019 og 2020 (NSM, 2016; NSM, 2017; NSM, 2018; NSM, 2019; NSM, 2020). Angrepene blir ofte rettet mot norsk næringsliv og offentlige interesser, som oljesektoren. Videre i risikovurderingen kommer det frem at disse angrepene kan ha stort skadepotensiale og kan i

løpet av kort tid kan ødelegge deler av viktig infrastruktur (NSM, 2013). For oljeselskaper handler dette om alt fra skader på installasjoner offshore til sikring av informasjon og konfidensialitet på lokasjonene på land.

Det har vært flere digitale angrep mot oljerelaterte selskaper. I Norge er nok det mest kjente angrepet som ble utført mot Norsk Hydro i mars 2019. Det er mye som indikerer at oljesektoren er et mål for ondsinnede aktører med ulike digitale angrepsmetoder (Lysneutvalget, 2015). Oljesektorens verdier og muligheten til å påføre store skader på utstyr og installasjoner gjør den til et attraktivt mål. PST (2020) skriver i sin sikkerhetsvurdering for 2020 at digital kartlegging og sabotasje av kritisk infrastruktur er blant de mest alvorlige truslene Norge står ovenfor. På spørsmålet om hvilke cybertrusler informantene mener at oljeselskaper i Norge står ovenfor i dag svarte de henholdsvis likt. Blant annet nevner alle informantene sosial manipulering som en cybertrussel. Dette går ut på at en person på innsiden av selskapet blir lurt til å oppgi sensitiv informasjon til en kriminell aktør. På denne måten kan aktøren få tilgang til informasjon om eksempelvis adgangskontroll.

De siste årene har det vært økt fokus på cybertrusler og hvilke enorme skader de kan utgjøre for ulike sektorer. Blant annet kommer det som nevnt i innledningen frem i NOU 2015:13 at digitaliseringen samfunnet har gått gjennom bidrar til å gjøre oss mer sårbare. Dette gjelder også for oljesektoren. Det finnes flere typer digitale sårbarheter i oljesektoren som alle bringer med seg svakheter som ondsinnede aktører kan unytte. Lysnesutvalget (2015) har lagt frem en liste over topp 10 digitale sårbarheter i oljesektoren:

1. Manglende oppmersomhet og opplæring hos de ansatte
2. Fjernarbeid
3. Bruk av standardprodukter med kjente sårbarheter i produksjonsmiljø
4. Mangelfull sikkerhetskultur hos underleverandører
5. Mangel på seperasjon av datanett
6. Mobile lagringsenheter
7. Datanett mellom landintallasjoner og oljefelt
8. Manglende fysisk sikring av datarom, kablingsskap, m.m.
9. Sårbar programvare
10. Utdaterte styresystemer på installasjoner

Tabell 5: Topp 10 sårbarheter i oljesektoren, (Lysnesutvalget, 2015).

Lysneutvalget (2015) skriver videre i sin rapport «Digitale Sårbarheter Olje & Gass» at all aktivitet i oljesektoren er forbundet med risiko, i økende grad gjelder dette også digital risiko. Det advares videre mot økning av digitale trusler mot norske virksomheter, hvor spesielt oljesektoren er utsatt. Dette kan en se igjen i at de større alvorlige angrepene de siste årene har gått hardt ut over oljesektoren, slik som angrepene mot Maersk og Norsk Hydro. Metodene de ondsinnede aktørene bruker blir i tillegg mer sofistikerte. Konsekvensen av de uønskede hendelsene er stort sett økonomiske, men både omdømme, miljøødeleggelse og menneskeliv er konsekvenser som i de mest ekstreme tilfellene kan bli utfallet av et digitalt angrep. I oljesektoren er det mange forskjellige aktører som arbeider sammen, dette gir også flere aktører tilgang til sensitiv informasjon og muligheten for eksponering gjennom en skadevare som eksempelvis en ondsinnet link fra en phishingmail.

I informantintervjuene var det flere forskjellige svar på hvilke cybertrusler oljeselskapene står

ovenfor. Oljenæringen er en næring mange er negative til og flere ønsker at oljenæringen skal avvikles. IN1 og IN3 dro først frem miljøaktivister og miljøvernorganisasjoner som aktører som kan være villige til å gjennomføre cyberangrep. «Vi har vurdert det slik at vi kan være et spesifikt mål, da vi driver en bransje som ikke alle liker» (IN3).

For IN2 var cyberangrep mot offshore kontrollsystem en av cybertrusselene de har mest fokus på grunnet det store skadepotensialet det kan påføre selskapet. I de aller verste tilfellene kan menneskeliv gå tapt. «Dersom en aktør klarer å hacke et kontrollsystem vil det få store økonomiske konsekvenser, men i verste fall kan det gå utover helse og sikkerheten til arbeiderne» (IN2). Som nevnt i *2.1 Oljesektoren og digitalisering*, kan menneskeliv gå tapt dersom kontrollsystemene havner i feil hender (Høydal, 2020).

IN1 trekker ulike trusselaktører frem som en stor trussel, ikke bare for oljeselskaper men også for Norge i et større bilde. Et angrep som rammer oljeselskaper hardt vil også påvirke store deler av Norge. Det finnes flere statlige aktører som både har kompetanse og verktøyet til å gjennomføre et alvorlig cyberangrep. IN1 nevnte videre at det er viktig å se på sin egen virksomhet som en større del av hele Norge. «I den forbindelse kan vi bruke det som et politisk verktøy til å påvirke beslutninger og kanskje også lande beslutninger i Norge». IN1 fortsetter med å forklare hvordan de kriminelle aktørene som gjennomfører et cyberangrep kan misbruke informasjonen de stjeler til seg. «De bruker informasjonen for å oppnå en form for vinning, de kan selge informasjonen videre, ødelegge infrastruktur, de kan låse opp, kuppe og blokke systemer. Ofte gjør aktørene dette for å kunne kreve løsepenger til å åpne systemene opp igjen» (IN1).

5.1.2 Phishing som en trussel for oljesektoren

Som nevnt i innledningen er phishing ikke en ny angrepsmetode, men fremdeles er det en av de mest brukte angrepsmetodene. Sommeren 2014 opplevde norsk olje- og energisektor et e-postangrep som var større enn noensinne. E-poster ble sendt ut til over 50 virksomheter i olje- og energisektoren med den baktanke om å lure mottakerne til å trykke på en ondsinnet link (NSM, 2015).

På spørsmålet om hvilken cybermetode informantene ser aller mest av var phishingangrep klart svaret hos alle tre. «Noen kan ønske å skade oss, forsøke å komme inn i systemet og

skade selskapet ved å ødelegge ting» (IN3). Deretter forklarte alle informantene at phishing var et sterkt fokusområde i deres selskap. Likevel kunne IN1 og IN2 fortelle at deres selskap hadde opplevd en uønsket hendelse relatert til phishing. IN2 forklarte at angrepet skjedde ved at en ansatt hadde trykket på en ondsinnet lenke. Lenken inneholdt en ransomeware som gjorde at alle filene på en spesifikk drive låste seg. Heldigvis ble det raskt oppdaget og hackeren fikk kun tak i 1 av 10.000 filer på den driven. Phishingangrepet mot selskapet til IN1 dreide seg også om at en ansatt uheldigvis trykket på en ondsinnet link. Også her ble angrepet avverget før det fikk store konsekvenser.

«Å oppleve et slik angrep som Hydro, det er skrekkscenarioet» (IN3)

Informantene går videre inn på målrettete phishingangrep. «I noen tilfeller kan det være målrettet, det vil si at man kartlegger personene på forhånd, hvilken posisjon de besitter, hvilken stilling de har også former man et skreddersydd budskap til personen» (IN1). Noen kan gjøre seg ekstra godt kjent med selskapet, og dersom ønsket er å skade selskapet kan kriminelle aktører komme seg inn i selskapet på et eller annet vis. For IN3 var målrettede angrep mot kontrollsystem et scenario som de arbeidet nøye med. Ofte hadde de også beredskapsøvelser hvor de øvde på hvordan de skulle håndtere en slik uønsket hendelse.

5.1.3 Nyansatte som en sårbar gruppe i oljesektoren

Som fremvist i tabell 5 ligger manglende oppmerksomhet og opplæring hos de ansatte på topp over topp 10 digitale sårbarheter i oljesektoren. Videre skriver Lysnesutvalget (2015) at phishingangrep oftest er grunnet menneskelig feil. Ansatte lures til å oppgi sensitiv informasjon og dette kan ha fatale skader for oljeselskapet. Derfor blir menneskelige feil ansett som den største digitale sårbarheten i oljesektoren. NSM (2017) skriver også at mennesker kan være et svakt punkt i selskapene de er ansatt i. Bevisstgjøring og holdningkampanjer er tiltak som kan bidra til å minske den digitale sårbarheten ansatte utgjør (NSM, 2017).

Ansatte kan unyttes av ondsinnede aktører til å gi tilgang til systemer, informasjon eller prosesser (NSM, 2018). Svakheter og mangler i selskapenes arbeid med personellsikkerhet kan bidra til å gjøre det enklere for ondsinnede aktører å gjennomføre angrep (NSM, 2019). Som nevnt i innledningen er Atea (2018) og Uninett (2013) blant de som trekker frem at phishingangrep mot nyansatte er noe vi bør se opp for i fremtiden. VadeSecure (2019) skriver

også at nyansatte det perfekte mål for et phishingangrep. Grunnen er at nyansatte er lite kjent med både folk og prosess i sitt nye arbeidsforhold. I tillegg til at nyansatte ønsker å gi et godt inntrykk og frykter å gjøre feil. I et phishingangrep kan ønsket om å svare raskt gjøre at den nyansatte overser kjennetegnene på en phishingmail, og blir lurt (VadeSecure, 2019). På mitt spørsmål om i hvilken grad informantene tror at nyansatte utgjør en større trussel var det flere interessante svar.

«Godt poeng! Det har vi ikke hatt fokus på, vi har nok tenkt at nyansatte ikke utgjør en spesielt større bekymring» (IN2).

«Det er nok en liten erkjennelse at vi har tenkt at nyansatte er veldig IT-kyndige. Men det er helt korrekt det du påpeker, de er en av mange og de har lyst å gjøre en god jobb. Du er på hele veien og kan lett gå på et slikt angrep» (IN3).

IN1 svarte derimot at selv om nyansatte er utsatt, er det ikke sikkert at de er mer utsatt enn etablerte ansatte. Dette begrunnet IN1 med at nyansatte ofte er yngre personer som har vokst opp i en digital verden. Dermed er oppfatningen at nyansatte besitter mer kunnskap om teknologien, dens utfordringer og trusler. Likevel avslutter IN1 med å si at «det eneste må være at man i en tidlig fase i ansettelsesforholdet er aller mest ukjent. Det dukker opp nye ting, nye linker og nye henvendelser om adganger. Man vet ikke helt, så man antar at man bare skal trykke på en link».

5.2 Hvorfor og hvordan spiller kunnskap og kompetanse inn på de ansattes forståelse av phishingangrep?

Opplæring

IN1 forklarte at phishing går mye ut på at den ansatte hverken har nok kunnskap om hvordan en kan bli utsatt for et angrep ei heller om hvilke konsekvenser et angrep faktisk kan føre til. Kunnskap og kompetanse om phishingangrep kommer blant annet gjennom opplæring og oppfølging av de ansatte. Alle informantene forklarte at de hadde en generell opplæring helt i starten av et ansettelsesforhold hvor de nyansatte skal gjennom kurs som omhandler datasikkerhet. IN2 forklarer at opplæringskurset har mye fokus på «beste praksis» ved bruk av IT. Eksempelvis hvor ofte en skal bytte passord, hvordan lage sikre passord og at de ansatte skal låse skjermen når de går fra arbeidsplassen. For IN1 sitt selskap M var opplæringen

forskjellig ut ifra hvor i selskapet den nyansatte skal jobbe, men legger til at de bruker en generell tilnærming i introduksjonsprogrammet for nyansatte. I selskapet til IN3 sier informanten at hos dem må nyansatte gjennom en stor del opplæring, kurs og trening. Kurs om cyber security er blant annet obligatorisk samtidig som resultatene måles og hvor de i slutten av opplæringen må gjennomgå en test hvor en får bestått/ikke bestått.

Ifølge Lysnesutvalget (2015) er holdningskampanjer og bevisstgjøring som omhandler digitale sårbarheter like viktig som fysiske barrierer. «Før var cyber security kurset påkrevd, nå er det valgfritt» (IN2). Til sammenligning har selskapet til IN2 et kurs om etikk som er obligatorisk. Likevel oppfordres de ansatte i selskapet til IN2 til å ta cyber security kurset, og om de ikke har tatt det vil lederen forsøke å gi klar beskjed om at alle i teamet bør ta kurset. Kurset inneholder viktig informasjon som eksempelvis fokus på cyber security på arbeidsplassen men også hjemme og på reise.

Oppfølging

IN3 kunne fortelle at i deres selskap har de et eget oppfølgingsvektøy hvor du melder deg på kurs. I tillegg kan ledere delegere kurs til sine teammedlemmer. På denne måten kan lederen følge med på at alle holder seg oppdatert og tar kursene. Gjennom informantintervjuene kom det også frem at alle informantene hadde et digitalt akademi hvor ansatte kan logge seg inn å ta ulike kurs og holde seg oppdatert. På disse sidene legges det ut videosnutter av for eksempel hvordan du kan rapportere inn en mistenkelig e-post.

Phishingkampanjer

Alle informantene kunne fortelle at de aktivt drev med phishingkampanjer. Da sender selskapet ut e-poster som skal etterligne ekte phishingmailer. Målet er å se i hvilken grad de ansatte trykker på linken, legger inn sensitiv informasjon eller om ansatte melder fra til IT om at de har mottatt en mistenkelig e-post. IN2 meddelte at 90% av de ansatte ikke hadde trykket på linken som selskapet med vilje sendte ut.

IN3 forklarte at de hadde et system hvor ansatte blir rangert på fem ulike nivåer ut fra hvordan de møter phishingmailene som blir sendt ut via kampanjen. Dersom en ansatt trykker på en link eller legger inn informasjon havner de nederst og må jobbe seg opp igjen på ranken. Videre forklarte informanten at phishingkampanjene skapte et fellesskap på

arbeidsplassen da de ansatte målte seg opp mot hverandre og skapte en slags intern konkurranse om å holde seg på det øverste nivået. Videre forklarte informanten at selv om de aller fleste er positive til phishingkampanjene er det noen ansatte som blir frustrerte over at selskapet prøver å «lure» dem til å trykke på en link. Informanten påpeker derimot at selskapets hyppige og spesifikke phishingkampanjer bidrar til å heve sikkerhetsnivået på generell basis.

5.3 Hvordan kan oljeselskaper arbeide for å redusere risikoen for at ansatte blir utsatt for et phishingangrep?

PwC (2019) forklarer at det er økt fokus på bevisstgjøring av ansatte i møtet med cyber security. Mange selskaper ser på dette som en høyt prioritert sikkerhetsinvestering. På spørsmål om hvordan selskapene arbeider for å hindre phishingangrep i dag svarte IN1 at de ønsker å bygge sikrere systemer som tar høyde for menneskelige feil. Disse systemene skal gjøre det vanskeligere for den ansatte å installere programmer ved at de tar vekk rettigheter fra den ansatte. «Phishingangrep ønsker å få deg til å trykke på en link slik at det installeres en skadevare» (IN1). Ved å ta i bruk systemer som tar høyde for dette kan en redusere sjansen for at skadevaren blir installert på datamaskinen.

«Vi må hele tiden tenke at noen kan ønske å skade systemet, selskapet eller personer» (IN3). For IN3 var det flere punkter som kunne bidra til å bedre arbeidet mot phishingangrep. Blant annet fortalte informanten at de hadde et obligatorisk kurs om sikring som måtte gjennomføres for alle nyansatte. Kurset måtte bestås før de nyansatte i det hele tatt fikk komme inn i bygget. Forslaget til informanten var at det samme burde blitt gjeldene for cyber security, nemlig et kurs som må godkjennes før nyansatte kan få PC med innloggingsdetaljer. «Vi må tenke sikring fra dag en». Informanten nevner også «security in design» som vil si at det bygges tekniske barrierer inn i alt utstyr. «Vi prøver å bygge systemer slik at de er sikre i design, at de ikke blir installert med virus».

Deling og læring

«Sharing er viktig!» (IN2). Informanten forteller om et forum hvor man kan dele hendelser eller erfaringer man har gjort seg og diskutere ulike tilnærminger til sikkerhet og cyber security. Videre forklarer informanten at det må bedre systemer til for måling av effekt, med dette menes effekt av kursene som blir sendt ut. «Hvor mange tar kursene, hvor mange

mangler å ta kursene? Og så videre». Samtidig påpeker informanten viktigheten av at kursene også følger teknologien. Teknologien utvikler seg raskt og det kommer stadig nye phishingmetoder. Derfor er det viktig at selskapet og kursene holder seg oppdatert. For IN2 var det derimot viktig å ikke bare kurse seg og se på hvordan en kan trene best mulig, men det er desto viktigere å faktisk ha en plan på hva en skal gjøre dersom de blir utsatt for et phishingangrep. «Det vil være viktig med table-top øvelser på cyberhendelser også». Med Table-top øvelser mener informanten øvelser hvor en sitter rundt et bord og diskuterer hvordan en skal reagere ved en eventuell phishinghendelse.

6.0 Diskusjon

I dette kapittelet vil de empiriske funnene i kapittel 5 bli diskutert og tolket gjennom valgte teoretiske perspektiv som er lagt frem i kapittel 3. Funnene vil også bli diskutert i lys av oppgavens innledning og tidligere forskning. Det bør også nevnes at noen av funnene blir brukt flere plasser, men til ulike formål. Kapittelet er strukturert etter forskningsspørsmålene slik som i foregående kapittel. Drøftingen leder tilslutt opp til kapittel 7, konklusjon av problemstillingen «*I hvilken grad utgjør nyansatte en større risiko for phishingangrep enn etablerte ansatte i oljesektoren?*»

6.1 Hvordan har oljesektoren erkjent og forholdt seg til phishing som en cybertrussel, og i hvilken grad har en fokusert på nyansatte som en sårbar gruppe i forhold til denne trusselen?

De siste årene har det vært økende fokus på digitale trusler og de enorme konsekvensene det kan ha for et stadig mer digitalisert samfunn. Fra 2015 til 2020 har PST i sin trusselvurdering trukket frem petroleumsnæringen som en kritisk infrastruktur. Lysnesutvalget (2015) er også blant dem som trekker frem oljesektoren som et mål for ondsinnede aktører. Dette innebærer at oljeselskaper er mulige ofre for blant annet cyberangrep. Trusler, verdier og sårbarhet er begreper som er sentrale innenfor risiko (Bergsjø, Windvik & Øverlier, 2020). Oljeselskaper har store verdier som en trusselaktør kan ønske å skade. I oljesektoren har store selskaper som Saudi Aramco, Maersk og Norsk Hydro opplevd omfattende cyberangrep. I disse tilfellene har en trusselaktør med evne, kompetanse og kapasitet utnyttet selskapenes sårbarhet til å gjennomføre et angrep med mål om å skade dens verdier

6.1.1 Phishing som en trussel for oljesektoren

Alle informantene trakk frem phishing som den cybertrusselen de så aller mest av. Dette gjenspeiles i NorSIS sin rapport om trusler og trender for 2019-2020 hvor phishingangrep ligger klart øverst. Phishingangrep kan gjennom enkle grep gjøre store ødeleggelser. Ved at ansatte uten vilje oppgir brukerinformasjon eller annen sensitiv informasjon kan en trusselaktører med få steg få tilgang til systemer og informasjon som kan skade selskapet i stor grad. At phishingangrep ses på som den største trusselen kan ha sammenheng med hvor lite som faktisk skal til for at et forsøk på phishingangrep blir vellykket. Dersom en

trusselaktør med teknisk innsikt, kompetanse og motivasjon sender ut en selskapsspesifikk e-post til et oljeselskap vil det ofte være nok at kun én person i dette selskapet blir lurt til å trykke på en ondsinnet link. I tillegg kan trusselaktøren sitte på andre siden av jordkloden, da det kreves ikke tilstedeværelse i form av fysisk kontakt med selskapet en ønsker å ramme. Dette gjør at phishing ikke har noen begrensninger for hvor eller hvordan det kan gjennomføres. Noe som igjen gjør trusselen enda større for oljesektoren.

NSM (2016) skriver at oljeselskaper må kunne vurdere sårbarhet og risiko som omhandler teknologi, organisasjon og mennesket. I informantintervjuene fremkommer det at både mennesket, teknologien de arbeider med, og organisasjonen en jobber i spiller en stor rolle i møtet med phishingangrep. Et argument er at jo større selskapet er jo flere personer kan være potensielle kilder til at et phishingangrep blir vellykket. I selskapene fra empirien er det forskjell i størrelse og antall ansatte. Det minste selskapet har naturlig minst antall ansatte, noe som bidrar til å redusere sjansen for at en ansatt trykker på linken. I det største selskapet er det flere ansatte og dermed også flere personer som uheldigvis kan bli offer for et phishingangrep.

Sidney Dekker (2006) viser til «The New View» og «The Old View» når det kommer til synet på menneskelige feil. «The Old View» viser som nevnt til at mennesket ene og alene er feilen hvis de eksempelvis trykker på en ondsinnet link, mens «The New View» ser på bakenforliggende årsaker til at ansatte trykket på linken. I lys av empirien er det «The New View» som er fremtredende hos oljeselskaper i Norge. Selv om det er mennesket som aktivt trykker på en ondsinnet link er alle informantene klare på at det er selskapet og deres manglende evne til å gi den ansatte god nok opplæring og oppfølging som blir kritisert og fulgt opp i etterkant av hendelsen. Her kommer også forskjellen mellom det minste og det største selskapet i empirien godt frem. Det største selskapet har en klart bedre opplæring og oppfølging. Selv om argumentet med at et større antall ansatte gir større sannsynlighet for at en ansatt trykker på ondsinnet link vil opplæring og oppfølging bidra til å redusere denne sannsynligheten. Det minste selskapet har på den andre siden mindre ansatte, men igjen en mindre god opplæring og oppfølging. Noe som gjør at sannsynligheten for at en av deres ansatte trykker på linken kan være større enn ved det største selskapet, på tross av at de er færre ansatte.

6.1.2 Nyansatte som en sårbar gruppe i oljesektoren

Lysnesutvalget (2015) og NSM (2017) skriver at menneskelig feil svært ofte er grunnen til at et phishingangrep blir vellykket. Svakheter med sikkerhetsarbeidet kan ifølge NSM (2019) bidra til å forenkle arbeidet til angriperne. Både VadeSecure (2019), Atea (2018) og Uninett (2013) trekker frem nyansatte som en sårbar gruppe i møtet med phishingangrep. Dersom en nyansatt får en e-post med mistenkelig innhold kan terskelen for å spørre andre ansatte eller sjefen om en vurdering muligens være høyere enn hos etablerte ansatte. Etablerte ansatte er godt kjent med selskapets rutiner, hvilke type mailer som vanligvis sendes ut og hvor de skal henvende seg dersom de mottar en mail med et mistenkelig innhold. Dette er faktorer som er med på å gjøre nyansatte mer sårbare enn etablerte ansatte i møtet med phishingangrep. På den andre siden trekker IN1 frem nyansatte som en yngre og mer datakyndig gruppe enn etablerte ansatte. Med dette mener informanten at de nyansatte ofte har bedre teknologisk innsikt og med dette vil være mer observant på blant annet phishingeposter. Derimot vil etablerte ansatte ofte representere en eldre gruppe som ikke har den samme teknologiske og digitale kompetansen som yngre mennesker.

6.1.3 Forståelse av phishingangrep

PwC sin Cybercrime Survey fra 2019 viser at ansatte og deres ubevisste handlinger er en stor trussel for selskaper. Phishingangrep er blant de hyppigste angrepsformene og hele 84% av respondentene i undersøkelsen hadde opplevd et slikt angrep. Gjennom intervjuene kommer det frem at hverken IN2 eller IN3 hadde hatt særlig fokus på nyansatte som en økt risikofaktor i møtet med phishing. Som nevnt tidligere hadde informantene et inntrykk av at nyansatte var yngre mennesker med god teknologiforståelse og datakyndighet. IN1 var den eneste av informantene som hadde et bevisst forhold til at nyansatte kunne utgjøre en større risiko og at en ikke må stole blindt på at nyansatte har god nok digital kompetanse. Selskapets sikkerhetsarbeid er en viktig faktor for å minske denne risikofaktoren. Boyesen (2003) skriver at hva den individuelle oppfatter som risiko og hvor risikofylt det oppleves styres av både individet men også kulturen individet er en del av. Gjennom arbeid med opplæring, oppfølging og oppdatert kunnskap kan selskapet bidra til en økt kompetanse hos sine ansatte. Den økte kompetansen hos nyansatte og etablerte ansatte er en viktig suksessfaktor for selskapet i etableringen av sikkerhetskultur for å styrke de ansatte i møtet med phishingangrep. I tillegg vil arbeidet kunne bidra til å minske skille mellom nyansatte og etablerte ansatte når det kommer til teknologiforståelse og digital kompetanse.

6.2 Hvorfor og hvordan spiller kunnskap og kompetanse inn på de ansattes forståelse av phishingangrep?

SecurityInnovation (u.å) skriver at de aller fleste selskapene tror at teknologiske løsninger skal kunne hindre blant annet phishingangrep mot deres ansatte. NorSIS (2020) nevner at tiltak som totrinnsbekreftelse, oppdaterte programvarer og antivirusbeskyttelse kan bidra til å forbedre sikkerheten. Dessverre er det ingen teknologi som kan ta høyde for alle mulige menneskelige feil og uaktsomhet. På bakgrunn av dette er opplæring, kunnskap og kompetanse viktige bidrag for å gi ansatte en forståelse av hva et phishingangrep er og hvordan man kan unngå det. Men hvordan arbeider selskapene med kunnskap- og kompetanseheving hos de ansatte? Og i hvilken grad bidrar kunnskap og kompetanse til å hindre phishingangrep?

6.2.1 Kunnskap og kompetanse

I oppgavens kapittel «*5.1.1 Cybertrusler i oljesektoren*» kan en lese at manglende oppmerksomhet og opplæring hos de ansatte ligger øverst på listen over digitale sårbarheter i oljesektoren (Lysnesutvalget, 2015). NSM (2017) skriver at bevisstgjøring og holdningskampanjer er tiltak som bidrar til å redusere sannsynligheten for at ansatte blir utsatt for et phishingangrep. Dette ses godt igjen i informantintervjuene, hvor en kan lese at selskapene driver med både opplæring og bevisstgjøring for å øke kunnskapen til de ansatte. NorSIS (2020) skriver at kunnskap og opplæring bidrar til å redusere sjansen for phishingangrep. IN1 trekker frem at phishingangrep går ut på at en ikke har nok kunnskap om hvordan man kan bli utsatt for det og hva det innebærer å trykke på lenker man mottar i e-poster. Alle selskapene arbeidet med å øke kunnskapen og kompetansen hos sine ansatte, likevel var tilnærmingsmåten og kvaliteten ulik.

Opplæring

SINTEF (2013) poengterer at dersom en ansatt skal få informasjon, kunnskap og kompetanse vil opplæring være en av de viktigste lærepunktene. Selskapene som ble brukt i oppgaven er som nevnt forskjellige i størrelse og omfang. IN3 jobber i det største selskapet som i tillegg er det selskapet med mest ressurser. Gjennom informantintervjuene kan en se at selskap L har et mer systematisk og godt gjennomarbeidet system for å øke kunnskap og kompetanse hos sine nyansatte. Opplæringen virker å være av høy kvalitet med tett oppfølging og gode rutiner.

Denne typen organisering og oppfølging krever at selskapet legger ned både tid og ressurser. På den andre siden har vi selskap S til IN2, som er det minste selskapet. Her har de gått for en annen tilnærming. Blant annet har kurset i cyber security tidligere vært pålagt mens det nå er frivillig. Selskapet har i tillegg vært utsatt for et phishingangrep og burde derfor vært klar over risikoen ved å ikke ha godt nok informerte ansatte når det kommer til phishing som en cybertrussel. I og med at selskapet er lite bør det i tillegg være overkommelig å sørge for at alle nyansatte får den innføringen og kursingen som kreves.

Kvaliteten av arbeidet med kunnskap og kompetanse har i dette tilfellet økt i takt med selskapets størrelse. Selskap L har kvalitet og kontinuitet på både opplæringen og oppfølgingen. Selskap S har i mindre grad et like systematisk og profesjonelt opplegg. Dette viser at selskapet og ressursene de innehar kan i stor grad påvirke kvaliteten på opplæringen som blir gitt. Et stort selskap som selskap L kan gå i fellen av å miste oversikt over nyansatte og dermed ikke ha like god opplæring eller tett oppfølging. Likevel viser empirien at selskapet har etablert gode rutiner og har en systematisk metode for å integrere nyansatte i selskapet og i selskapets policys. For selskap S bør de i utgangspunktet kunne ha en god og tett innkjøring for nyansatte, da de er et mindre selskap. I et mindre selskap kan en se for seg at nyansatte blir mer lagt merke til og derav får en mye tettere oppfølging. Likevel viser informantintervjuene i dette tilfellet at kvaliteten på opplæringen av nyansatte er merkbart høyere hos selskap L enn hos selskap S.

I Ptil (2011) sin §22 «opplæring i sikkerhet og arbeidsmiljø eller arbeidsmiljøloven» kommer det frem at sikkerhet er et av områdene hvor ansatte skal få opplæring. Videre står det i §22 at opplæring er lederen sitt ansvar. IN2 forklarte i den forbindelse at lederen blir varslet dersom den ansatte ikke har tatt cyber security kurset. Deretter blir det lederens ansvar å oppfordre den ansatte til å gjennomføre kurset. Likevel har ikke lederen i dette tilfellet myndighet til å kreve at kurset skal bli gjennomført av den ansatte. NSM (2015) poengterer også at sikkerhet- og beredskapsarbeidet er et lederansvar. I sammenheng med dette forklarte IN3 at i deres selskap ble leder varslet dersom en ansatt hadde blitt «lurt» av phishingkampanjene i regi av selskapet. Den ansatte ble da kalt inn til møte med lederen som skulle identifisere hvorfor den aktuelle ansatte ikke oppdaget phishingforsøket i kampanjen. I dette tilfellet kan en se at den ansattes kunnskap og kompetanse også er et lederansvar. Her får den ansatte tett oppfølging og lederen tar en større del i oppfølgingen for å styrke den ansatte, som igjen vil bidra til å styrke selskapet.

IN1 i selskap M forklarte at opplæringen og godheten av den ofte var avhengig av hvilken avdeling i selskapet du kom inn i. Som nevnt kan ingen teknologi ta høyde for alle typer menneskelige feil, og menneskelige feil kan skje over alt i selskapet. En tilnærming hvor ulik opplæring blir gitt i ulike deler av selskapet kan potensielt utgjøre en sårbarhet. Ondsinnede aktører kan i dette tilfelle utnytte svakheten i selskapet ved å etablere hvilke avdelinger som har en mindre god opplæring. På bakgrunn av denne informasjonen kan den ondsinnede aktøren sende en phishingmail til den delen av selskapet med svakest opplæring og dermed øke sjansene for et vellykket phishingangrep. For alle selskapene i empirien vil kunnskap og kompetanse om phishing som fenomen samt konsekvensene av et eventuelt angrep gjøre de ansatte bedre rustet til å kunne håndtere eller unngå et phishingforsøk uavhengig av avdeling. Opplæringen vil i stor grad være avgjørende for selskapet i deres evne til å oppdage og håndtere et phishingangrep.

Fra informasjon til kunnskap

Det finnes flere måter en kan informere ansatte om hvilke ulike phishingmetoder som finnes i tillegg til hvilke konsekvenser et vellykket phishingangrep kan gi. Filstad (2010) påpeker viktigheten av å utvikle informasjon til kunnskap. Informasjon forblir bare informasjon når det ikke blir anvendt gjennom handling. Når informasjon blir anvendt gjennom handling vil det kunne generere kunnskap og kompetanse. Gjennom informantintervjuene kommer det frem at alle selskapene aktivt driver med phishingkampanjer. Filstad (2010) skriver videre at kunnskapen blir til når mennesker blant annet reflekterer. Det er nettopp bruken av egen refleksjon selskapene forsøker å få frem i bruken av phishingkampanjer.

IN3 nevnte at flere ansatte tenker at selskapet er ute etter å «lure» dem gjennom phishingkampanjene. Flere ansatte satte spørsmålstegn ved hvorfor selskapet med vilje ønsket å lure de ansatte til å trykke på linker. Som et motsvar påpekte informanten viktigheten med at phishingkampanjene får ansatte til å tenke og reflektere over mailene de mottar. Filstad (2010) forklarer nemlig at for å utvikle informasjon til kunnskap er det nødvendig at både kropp og hjerne tas i bruk ved hjelp av interaksjon og refleksjon. Når en ansatt mottar en phishingmail sendt fra selskapet vil det kreve både oppmerksomhet, interaksjon, refleksjon og beslutningsevne. Alle disse faktorene er med på å aktivere kroppen og hjernen. Som ansatt blir du satt på prøve i håp om å oppdage noe ved mailen som gjør at du reagerer. Det kan være alt fra skrivemåte, skrivefeil eller typiske kjennetegn som at mailen spør om

kontonummer eller brukerinformasjon. En slik vurdering vil kreve nettopp oppmerksomhet, interaksjon, refleksjon og beslutningsevne.

SINTEF (2013) forklarer at selskaper er nødt til å omstille seg i takt med de teknologiske endringene. I tillegg advarer NSM (2010) mot angrepsmetoder via internett og påpeker at slike angrepsmetoder vil utgjøre en stor trussel. Sammen med de digitale endringene kommer også nye angrepsmetoder. Gjennom informantintervjuene kommer det frem at selskapene var opptatt av å følge med på ulike trusler og trender når det gjaldt cyberangrep. IN1 forklarte at det var viktig med oppdatert informasjon og kunnskap om trusselen. Oppdatert informasjon og kunnskap kan bidra til at selskapet hele tiden er klar over hvilke phishingmetoder som blir brukt og formidler dette ut til sine ansatte. IN3 sitt selskap var særlig opptatt av at phishingkampanjene som ble sendt ut ikke skulle være i samme format men med forskjellig utseende og budskap. Dette er med på å vise ansatte at phishing ikke er én spesiell type metode. Ulike phishingmetoder er stadig i endring og blir ofte inspirert av ting som speiler samfunnet.

6.2.2 Læring

Læring er viktig for å heve organisasjonens kunnskapsnivå om phishingangrep, og ifølge Fusemail (2017) vil et høynet kunnskapsnivå bidra til et høynet beskyttelsesnivå for hele selskapet. Argote og Ophir (2002) forklarer organisasjonslæring som en prosess hvor organisasjoner gjør endringer som følge av læring. IN3 sitt selskap L kommer her frem som et godt eksempel. De har ikke opplevd et phishingangrep selv, men informanten påpeker viktigheten av å ta lærdom fra Norsk Hydro sitt phishingangrep i 2019. Det viser at informanten sitt selskap har valgt å ta i bruk en «hindsight» dimensjon. Dette gjøres ved å bruke angrepet mot Norsk Hydro som en måte for å tilegne seg kunnskap og utvikle ny kompetanse om arbeid for å hindre phishingangrep mot eget selskap.

Selskap S har brukt «foresight» dimensjonen som en læringsstrategi. Informanten viser her til hvordan de ønsker å rette fokus på hvordan en skal reagere dersom et phishingangrep oppstår, altså hvordan de kan lære for å være bedre rustet i fremtiden. Hva skal gjøres, hvem skal gjøre hva og hvordan skal det gjøres, ved å tenke gjennom dette på forhånd mener informanten at selskapet vil være bedre rustet til å håndtere et potensielt angrep. Informanten forklarte videre at i deres selskap gjorde de en «table-top» øvelse, som innebærer at du må bruke interaksjon og refleksjon. Som Flistad (2010) skriver er dette helt avgjørende for å kunne utvikle

informasjon til kunnskap. Informanten tar her utgangspunkt i hendelser som kan skje i fremtiden og bygger robusthet i selskapet ved å være forberedt på hendelser som potensielt kan skade selskapet fremover i tid. I tillegg poengterer informanten viktigheten av «sharing is caring», hvor poenget er å dele håndteringen av eksempelvis et phishingangrep for at andre selskap skal lære og unngå en lignende hendelse i fremtiden. Dette vil være en «hidsight»-læringsdimensjon, der målet er at en skal lære av tidligere hendelser. Informanten forklarte at oljesektoren hadde diverse forum hvor man kan dele og lære av hverandres uønskede hendelser. På denne måten jobber oljesektoren sammen for en felles kunnskapsheving uavhengig av hvilket selskap man jobber i. Dette bidrar til et samlet høynet sikkerhetsnivå for oljesektoren som helhet.

6.2.2 High Reliability Organization

Et oljeselskap blir ofte betegnet som en HRO organisasjon. Ifølge Engen et al (2016) er det en høyteknologisk organisasjon som opplever svært få og alvorlige hendelser. Oljeselskaper i et HRO-perspektiv har fokus på kunnskap og kompetanse. For at disse fokusområdene faktisk blir etterfølgt vil det være viktig at organisasjonen arbeider godt med sikkerhetsarbeid både for nyansatte og etablerte ansatte. Som nevnt i kontekstkapittelet blir oljesektoren betraktet som en sektor med høyt fokus på teknologi og digitalisering, samtidig som de kontinuerlig arbeider for å optimalisere sikkerheten. Dette vises også igjen i informantintervjuene hvor blant annet IN2 nevner at deres selskap er opptatt av å sikre kontrollsystemene offshore, da dette kan ha katastrofale konsekvenser i form av tap av menneskeliv dersom en opplever et phishingangrep. I tillegg sier IN3 at de fokuserer på «security in design», som vil si at de tenker sikring helt fra første gang noe installeres. Selskapene arbeider med å få til nye teknologiske løsninger samtidig som de fokuserer på sikkerhet, noe som er i tråd med en HRO-tankegang. Denne arbeidsmåten bidrar til å styrke forebyggingen av uønskede hendelser samtidig som det vil være en viktig faktor for å begrense eventuelle konsekvenser.

I en HRO-tankegang skal ifølge Aven et al (2018) industrien kunne utvikles som pålitelig, noe som gjøres gjennom fire betingelser. Den første er sikkerhet og pålitelighet, hvor tanken er at begge deler skal ha høy prioritet i alle ledd av organisasjonen. For selskap M til IN1 kan det virke som at det ikke er tilfelle, da opplæring og fokus på cyber security var ulik avhengig av hvor i selskapet du kommer inn som nyansatt. Hos IN2 har kurset om cyber security som nevnt gått fra å være obligatorisk til å være valgfritt, dette kan også vitne om at cyber security

ikke har så høy prioritet som det burde. For IN3 var det litt annerledes, der skulle alle gjennom samme kurs, uavhengig av hvor i selskapet du skulle begynne å jobbe. Dette viser at selskap L sitt sikkerhetsfokus er gjennomgående i hele selskapet.

Den andre betingelsen er redundans. Redundans er med på å øke sikkerheten ved å kompensere for feil. Gjennom informantintervjuene kom det frem at alle selskapene innehar teknologiske løsninger som for eksempel brannmurer eller to-trinns pålogging. Disse teknologiske løsningene skal bidra til å øke sikkerheten hos selskapet. IN1 forklarte at det er endel tiltak som ligger i arkitekturen bak systemene som de ansatte ikke legger merke til. Det er her trafikken overvåkes. Dermed finnes det redundans i systemene som skal kompensere for at en ansatt trykker på en ondsinnet link. Redundansen ligger i at teknologiske systemer skal fange opp hendelsen og stanse angrepet fra å utvikle seg.

Den tredje betingelsen er desentralisert styring, organisasjonskultur og læring. Her er fokuset blant annet på å oppmuntre ansatte til å rapportere inn avvik eller mistanker om feil. Alle informantene oppga at de hadde mailsystemer som var designet for å kunne rapportere inn e-poster som de mistenkte var phishing. Spesielt i selskapet til IN2 kan en lese i empirien at de hadde fått et nytt verktøy hvor du kan rapportere inn en mistenkelig e-post direkte til vurdering hos hovedkontoret som har åpent 24/7. Dette er også en mekanisme som hjelper selskapet til å oppdage og lære om ulike typer phishingeposter og gjerne raskere kan etablere en forståelse for nye phishingmetoder. På denne måten kan selskapene være tidlig ute med å advare alle sine ansatte mot lignende phishingeposter.

Den siste betingelsen er organisatorisk læring, det innebærer å lære av feil, teste løsninger og prøve/feile. Gjennom informantintervjuene kommer det frem at alle selskapene har enten brukt hendelser i eget selskap som læring eller tatt læring av andre selskaper som har opplevd uønskede hendelser. Tilstedeværelsen av de fire betingelsene bidrar til å gjøre selskapene pålitelige og at det virker som tiltenkt selv i et høyteknologisk system.

6.3 Hvordan kan oljesektoren arbeide for å redusere risikoen for at ansatte blir utsatt for et phishingangrep?

Som nevnt i «*2.1 Oljesektoren og digitalisering*» har oljenæringen tidligere opplevd cyberangrep og den nye forskningsrapporten til TrendMicro advarer også mot kommende

angrep (Trend Micro, 2019). NSM (2015) sendte i tillegg ut en advarsel til olje- og energisektoren om at det vil komme forsøk på dataangrep. Samtidig nevner PST (2020) i sin trusselvurdering at de regner med at norske virksomheter kommer til å bli utsatt for ondsinnede nettverksangrep. Hvordan kan oljeselskapene arbeide for å redusere sannsynligheten for at de blir utsatt for et phishingangrep? Og hvordan kan de på best mulig måte hindre at ansatte blir utsatt for phishingangrep?

6.3.1 Opplæring

Naisbitt (1982) skriver at vi drukner i informasjon men tørster etter kunnskap. Det forklares med at utviklingen fra informasjon til kunnskap går gjennom å bruke informasjonen aktivt. Aktiv handling vil kreve at de ansatte reflekterer over vurderingene de gjennomfører. Gjennom informantintervjuene kommer det frem at alle informantene gir tilbud om opplæringskurs i cyber security til nyansatte, deretter blir informasjonen fra kurset omvendt til kunnskap gjennom gjentatte phishingkampanjer. Selskapene har ansvar for å transformere informasjon til kunnskap for sine ansatte. Utviklingen skjer gjennom å bruke informasjonen de ansatte fikk under opplæringen i aktiv handling. Dette gjøres blant annet gjennom phishingkampanjer, kurs og tester. Denne formen for aktiv handling kan bidra til at informasjonen som blir brukt underveis i lengden bidrar til å utvikle kunnskap og kompetanse hos de ansatte.

Den digitale utviklingen og metodene som brukes for å gjennomføre ondsinnede handlinger er hele tiden i fremdrift. Nye teknologiske løsninger og påfølgende nye sårbarheter skaper et kappløp mellom de ondsinnede aktørene og oljeselskapene. Kappløpet går ut på at ondsinnede aktører ønsker å finne nye metoder som oljeselskapene ikke er kjent med og dermed minskes sannsynligheten for at selskapene oppdager angrepene. Er derimot informasjonen er oppdatert i henhold til nye phishingmetoder samt følger den teknologiske utviklingen vil det gi et bedre utgangspunkt for de ansatte i møte med et phishingangrep. Dersom opplæringen er mangelfull vil det være vanskeligere for den ansatte å forstå phishing som metode i tillegg til å ikke ha informasjon om hvilke konsekvenser det kan få for selskapet dersom personen trykker på en ondsinnet link. Full informasjon om phishing som fenomen og konsekvensene det kan gi gjør dermed de ansatte bedre rustet til å anvende informasjonen i praksis. I tillegg til at selskapet blir bedre rustet som en følge av at de ansatte forstår konsekvensene av å trykke på en ondsinnet link og dermed er mer fokuserte i møtet med en mistenkelig e-post. På denne måten kan de ansatte i mindre grad bidra til å øke risikoen for at selskapets verdier blir skadet i

møtet med et phishingangrep. Istedenfor bidrar de ansatte til å øke robustheten til selskapet og minsker sannsynligheten for et vellykket phishingangrep.

6.3.2 Sikkerhetskultur

For oljeselskaper som høyteknologiske selskap er kontinuerlig fokus på sikkerhet et viktig aspekt av arbeidshverdagen. Dette kan vi se igjen i tankegangen om at oljeselskaper opererer som en HRO. Både IN2 og IN3 forklarte at de arbeider med «sikkerhet i design», som betyr at nye teknologiske løsninger og systemer skal bygges med et sikkerhetsfokus. Det vil si at en skal tenke sikkerhet fra første stund og unngå å bygge nye systemer med åpenbare sårbarheter som ondsinnede aktører kan utnytte. En god digital sikkerhetskultur innebærer evnen til å beskytte selskapets digitale verdier fra ulike trusler og trusselaktører (Bergsjø, 2020).

Et eksempel som IN3 dro frem var tanken om å innføre strengere adgangskontroll for nyansatte når det kommer til PC tilganger. Forslaget gikk ut på at nyansatte måtte bestå IT-kurs for å få tilgang til en PC. Tanken bak forslaget var at nyansatte tidlig får tatt del i selskapets policys og rutiner når det kommer til digital sikkerhetskultur. NorSIS (2019) legger frem åtte kjerneområder som er viktige for å bygge en digital sikkerhetskultur, to av faktorene er risikoforståelse og kompetanse. Gjennom forslaget til IN3 blir begge disse faktorene fokusert på allerede før den nyansatte får brukertilgang. På denne måten vil den nyansatte ha fått et innblikk i selskapets digitale sikkerhetskultur samtidig som at de digitale truslene selskapet står ovenfor har blitt kartlagt og forklart. En slik praksis kan virke som et forebyggende tiltak for å øke nyansattes robusthet i møtet med phishingangrep i sine første arbeidsuker.

PST (2015) skriver at en god sikkerhetskultur vises i den ansattes atferd. Sikkerhetskultur forklares videre av NSM (2014) som den kunnskap, motivasjon, holdning og adferd de ansatte besitter. Gjennom informantintervjuene kan en se at IN3 sitt selskap arbeider godt med sikkerhetskulturen i selskapet. Dette gjenspeiles i rangeringen av ansatte i forhold til phishingkampanjene. Selskapet til IN3 rangerte anonymt de ansatte i henhold til om de ble «lurt» av phishingkampanjen eller ikke. Rangeringen kan bidra til å øke motivasjonen hos de ansatte for å opparbeide seg mer kunnskap om phishing som fenomen. I tillegg nevnte informanten at rangeringen bidrar til et fellesskap for selskapet ved at det jevnlig diskuteres og snakkes om hvor de ulike ansatte ligger på rangeringen. Selv om rangeringen kun er

tilgjengelig for den aktuelle ansatte og deres leder var det stor åpenhet blant de ansatte selv om hvor de lå i forhold til de ulike nivåene. Dette kan bidra positivt til holdningen og adferden hos de ansatte ved å motivere dem til å ikke havne lavere på rangeringen enn sine kollegaer. På motsatt side kan konkurransen bidra til et usunt konkurranseforhold hvor en blir sett ned på dersom en ikke ligger øverst på rangeringen eller den ansatte kan bli sett på som mindre intelligent. Dette er faktorer som kan skape en dårlig sikkerhetskultur. Likevel er helhetsoppfatningen etter informantintervjuet at rangeringen av ansatte nesten utelukkende har bidratt til økt motivasjon og søken etter mer kunnskap om phishing hos de ansatte.

Adferd knyttet til sikkerhet sier noe om sikkerhetskulturen i et selskap. Reason (1997) forklarer sikkerhetskultur som et resultat av de verdiene og holdningene som personene besitter. Gjennom informantintervjuene kommer det frem flere arbeidsmetoder som bidrar positivt til sikkerhetskulturen. Blant annet var alle selskapene opptatt av å legge til rette for og oppfordre ansatte til å rapportere mistenkelige e-poster. Rapporteringen gjelder uavhengig av om det var en phishingkampanje eller et reelt angrep. Det overordnede ønsket var at terskelen for å rapportere inn skal være lav og de ansatte skal alltid oppmuntres til å rapportere inn og si ifra. En god sikkerhetskultur vises også igjen i selskapets evne til å lære av feil og arbeide mot at slike feil skal skje igjen (Reason, 1997). Spesielt for IN3 var det viktig å lære av Norsk Hydro sitt angrep. I tillegg var alle selskapene opptatt av å dele informasjon og lære av feil på tvers av oljesektoren. Tilslutt vil god sikkerhetskultur også innebære at selskapet er åpent for å gjøre endringer (Reason, 1997). En fleksibel kultur innad i selskapet vil gi dem bedre forutsetninger til å endre seg og bli mer motstandsdyktige i kampen mot phishingangrep. Gjennom informantintervjuene kom det frem at hverken IN2 eller IN3 hadde vurdert nyansatte som en større sårbarhet i møtet med phishingangrep. I etterkant av intervjuene påpekte likevel begge informantene at problemstillingen var interessant og at de ønsket å ta dette videre internt i selskapet. Dette vitner om at selskapene er åpne og tilpasningsdyktige

6.3.3 Menneske teknologi og organisasjon

Menneske, teknologi og organisasjon er tett bundet sammen i en stadig mer digitalisert oljesektor. Selv om oljenæringen blir mer teknologirettet skriver Ptil (2019) at det fremdeles vil være behov for både menneske og organisasjon til å etterstrebe krav og overvåke systemene. Eksempelet fra informantintervjuene om «sikkerhet i design», hvor en bygger designet sikkert fra første stund, viser viktigheten av samspillet mellom menneske, teknologi

og organisasjon. Dersom en ønsker sikker teknologi krever det menneskelig innblanding i tillegg til det organisatoriske aspektet som innebærer organisering, planer og retningslinjer. I et MTO-samspill er det disse tre faktorene som sammen gjør at vi kan sikre oss mot ulykker, samtidig som det også er årsaken til ulykker. Teknologisk kan en svikt eksempelvis være at en brannmur svikter og ikke fanger opp et phishingforsøk. En organisatorisk svikt kan være mangelfull opplæring, slik som vi kan se i selskapet til IN2 hvor cyber security kurset gikk fra å være pålagt til å bli valgfritt. Tilslutt vil en menneskelig svikt være at en enkelt ansatt trykker på phishinglinken. Denne typen menneskelig svikt har både selskap S og selskap M opplevd. Heldigvis var den menneskelige faktoren også positivt tilstede i form av at en oppdaget angrepet og dermed fikk muligheten til å avgrense konsekvensene.

Ifølge Stranden (2019) er organisasjonen selve limet mellom mennesket og teknologi, da de legger retningslinjer for databruk og tilgang hos nyansatte og etablerte ansatte i selskapet. Bento (2001) poengterer også at driften i et oljeselskap påvirkers i stor grad av organisatoriske forhold og menneskelige presentasjoner. Ikke bare skal organisasjonen sørge for god opplæring og tett oppfølging, men også teknologiske hindringer som gjør at den ansatte ikke trykker på en ondsinnet link. Informantene trakk alle frem teknologiske utfordringer, som eksempelvis svake brannmurer eller at ansatte får for mange tilganger og kan laste fritt ned fra egen datamaskin. Slike teknologiske svakheter kan bidra til at selskapene blir mindre robuste i møtet med phishingangrep. Derimot kan robuste teknologiske barrierer også være grunnen til at et phishingangrep blir oppdaget og fjernet.

6.3.4 Personellsikkerhet

NSM (2019) beskriver personellsikkerhet som de tiltak, handlinger og vurderinger som gjøres for å hindre at personell utgjør en sikkerhetsrisiko. Tidligere i oppgaven står det skrevet om ulike tiltak og vurderinger som kan gjøres for å redusere sannsynligheten for at en ansatt blir utsatt for et phishingangrep. Eksempler på tiltak og vurderinger er introduksjonskurs, opplæring, oppfølgning og kampanjer i regi av selskapene. Dette er tiltak og vurderinger som var gjennomgående hos alle informantene. Gjennom oppgaven kan en derimot se at kvaliteten på tiltakene og vurderingene var forskjellige hos ulike selskapene. Både opplæring, kvalitet på phishingkampanjer og strukturering av oppfølging ble praktisert på ulike måter. Eksempelvis hadde IN1 sitt selskap hadde ulik opplæring i ulike deler av selskapet. IN2 sitt selskap hadde endret cyber security kurset fra obligatorisk til frivillig. Mens IN3 sitt selskap på den positive siden hadde en god struktur på sin oppfølging av phishingakampanjer. Personellsikkerhet er

viktig for alle selskaper som har verdier som de ønsker å beskytte (Stranden, 2019). Dersom en ikke fokuserer på personellsikkerhet med påfølgende tiltak, handlinger og vurderinger av ansatte og deres sikkerhetsrisiko kan risikoen for at nyansatte blir utsatt for phishingangrep øke og dermed utgjøre en større sikkerhetsrisiko enn nødvendig. En økt sikkerhetsrisiko bidrar også til økt risiko for å skade selskapets verdier. Derfor er arbeidet med opplæring og oppfølging viktig for å redusere ansattes sikkerhetsrisiko i møtet med phishingangrep.

7.0 Konklusjon

Denne oppgaven har bidratt til å belyse phishing som en digital trussel mot nyansatte i oljesektoren. Videre har oppgaven fokusert på i hvilken grad nyansatte utgjør en større trussel enn etablerte ansatte i møtet med phishingangrep. I tillegg har oppgaven undersøkt hvordan oljeselskaper kan arbeide for å hindre et phishingangrep og hvilke faktorer er viktige å fokusere på. Flere aspekter har vist seg å være uavhengig av sektor og utfordringene kan generaliseres til flere forskjellige sektorer. Følgende problemstilling er lagt til grunn i oppgaven:

I hvilken grad utgjør nyansatte en større risiko for phishingangrep enn etablerte ansatte i oljesektoren?

I en stadig mer digital verden, med nye teknologiske løsninger og digitale nyskapninger blir også sikkerheten satt på prøve. I et hav av muligheter følger det også med sårbarhet og usikkerhet. På bakgrunn av oljenæringen og dens fremtredende teknologiske utvikling har jeg i denne oppgaven sett på digitale sikkerhetsutfordringer, med spesielt fokus på phishing. I oppgaven kommer det frem at alle informantene har en felles oppfattelse om at phishing er den cybertrusselen oljeselskaper i Norge ser desidert mest av. Når det kommer til phishingangrep mot nyansatte viser oppgaven at selv om nyansatte ofte er yngre med god teknologisk innsikt utgjør de likevel en risiko i begynnelsen av arbeidsforholdet. Ønsket om å gjøre et godt inntrykk og ha en god responstid, i tillegg til at de ikke er kjent med selskapet og dens policy er faktorer som bidrar til at en nyansatt uten vilje kan bli offer for et phishingangrep. Tidlig i fasen av det nye arbeidsforholdet mottar nyansatte store mengder informasjon på e-post og det er i denne perioden den nyansatte er mest utsatt. Underveis i arbeidsforholdet vil derimot denne risikoen flate seg ut og selskapets opplæring og oppfølging spiller en stor rolle for den ansattes adferd i møtet med phishingangrep.

Studien viser at opplæring er viktig for å jevne ut risikoen på en god og effektiv måte. Det innebærer at de nyansatte får en opplæring som er oppdatert og tilstrekkelig. Videre i arbeidsforholdet er oppfølging og oppdatering av kunnskap og kompetanse viktige faktorer for å kunne hindre phishingangrep. Teknologien utvikler seg og selskapene må følge med på trender og igjen videreføre denne informasjonen til sine ansatte. Deretter er det viktig å holde kunnskapen ved like eksempelvis ved kurs, kampanjer og konferanser, slik at de ansatte hele

tiden er klar over hvilke phishingmetoder som kan bli brukt mot dem.

Med det til grunn konkluderer jeg med at nyansatte i større grad utgjør en risiko for phishingangrep enn etablerte ansatte i starten av et ansettelsesforhold. Likevel jevnes denne risikoen ut og det kontinuerlige arbeidet med kunnskap og kompetanse for de ansatte spiller en stor rolle for selskapets robusthet i møtet med et phishingangrep. En kan si at kvaliteten på de organisatoriske forholdene og menneskelige presentasjonene samt de teknologiske kvalitetene har stor betydning for selskapet og arbeidet med fravær av vellykkede phishingangrep.

7.1 Forslag til videre forskning

Det er forhold i dette studiet som kunne blitt ytterligere utdypet og flere aspekter hadde vært interessante å gå mer i dybden på. I denne oppgaven er det fokusert på i hvilken grad nyansatte utgjør en større risiko for phishingangrep enn etablerte ansatte i oljesektoren. Først og fremst hadde det vært interessant å få empiri fra flere selskaper og på den måten kunne ta et enda større dypdykk i den nåværende problemstillingen. Det finnes svært få studier og rapporter om phishingangrep mot nyansatte med fokus på oljesektoren.

Sett bort fra dette er det flere interessante funn gjennom oppgaven som hadde vært nyttig å studere nærmere i fremtiden. Det første er effekten og godheten av phishingkampanjene. En kan lese gjennom hele oppgaven at alle tre selskapene driver aktivt med phishingkampanjer for å øke bevisstgjøringen hos sine ansatte og lære dem mer om phishing gjennom praktisk deltakelse. Phishingkampanjene gjør at de ansatte blir oppmerksom på når de har «blitt lurt» av en phishingmail sendt fra selskapet, i tillegg til at de får beskjed dersom de har oppdaget og rapportert inn en phishingmail. For at phishingkampanjene bedre skal kunne bidra som et risikoreduserende tiltak er det viktig at phishingkampanjene er oppdaterte og fremstår som tilsynelatende reelle. En interessant studie ville vært å sett på godheten av kampanjene, effekten det har på de ansattes risikoforståelse og i hvilken grad kampanjene bidrar til å minske sannsynligheten for vellykkede phishingangrep hos oljeselskapene.

Tilslutt nevner alle informantene «social engeneering», på norsk oversatt til «sosial manipulering», som en voksende trussel. Det handler om hvordan mennesker kan bli hacket og manipulert. Målet er å lure en person til å utgi sensitiv informasjon for så å utnytte denne informasjonen til å få tilgang til nettverk, systemer eller presse selskapet for penger. På

bakgrunn av dette hadde det vært interessant å se på hvorvidt sosial manipulering er et voksende fenomen og i hvilken grad ulike sektorer og kritiske samfunnsfunksjoner arbeider med å hindre slike angrep.

8.0 Litteraturliste

Aase, T. H., Fossåskaret, E. (2014) Skapte virkeligheter. Om produksjon og tolkning av kvalitative data. (2) Oslo: Universitetsforlaget.

Argote, L. og Ophir, R. (2002): Intraorganizational learning. Chapter 8 in Baum, J.A.C. (ed.): The Blackwell Companion to Organizations. Oxford: Blackwell.

Andersen, S.S (2006) *Aktiv informantintervjuing.* Oslo: Universitetsforlaget.

Aven, T., Boyesen, M., Njå. O., Olsen, K.H., Sandve, K. (2018) *Samfunnssikkerhet* (8.utg) Oslo: Universitetsforlaget

Aven, T., Renn, O. (2010). *Risk Management and Governance: Concepts, Guidelines and Applications. Springer*. ISBN 978-3-642-13925-3. 278 s.

Bartnes, M., (2006) *Safety vs. security.* SINTEF

Bento, J.P (2001) *Menneske – Teknologi – Organisasjon. Veiledning for gjennomføring av MTO-analyser.* Oversatt av Statoil. Petroleumstilsynet.

Bergsjø, H., Windvik, R., Øverlier, L. (2020) *Digital sikkerhet. En innføring.* Universitetsforlaget.

Blaikie, V & Priest, J. (2019) *Designing social research* (3. utgave) UK&USA: Polity press

Boyesen, M. (2003) *Risikopersepsjon – en innføring i fagfeltet.* Direktoratet for sivilt beredskap. Oslo.

Danermark, B., Karlsson, J. C., Jakobsen, L., Ekstrom, M. (2002) *Explaining Society: An Introduction to Critical Realism in the Social Science*s (Critical Realism: Interventions) 1st Edition. London & New York: Routledge.

Dekker, S. (2006). The Field Guide to Understanding Human Error. Ashgate. Lund University, Sweden.

Engen, O. A. H., Kruke, B. I., Lindøe, P. H., Olsen, K. H., Olsen, O. E. & Pettersen, K. A. (2016). *Perspektiver på samfunnssikkerhet*. Oslo: Cappelen Damm Akademisk.

Filstad, C. (2010). Organisasjonslæring – fra kunnskap til kompetanse. Bergen: Fagbokforlaget Vigmostad § Bjørke AS.

Garvin, D.A. (1993) Building a Learning Organization. Harvard Business Review, 71, 78-91.

Gressgård, L.J., Melberg, K., Risdal, M., Selvik, J.T., Skotnes, R.Ø. (2018) *Digitalisering i petroleumsnæringen. Utviklingstrender, kunnskap og forslag til tiltak.* IRIS

Holme, I. M., & Krohn, B. S. (1998). Metodevalg og metodebruk. Oslo: TANO

Holme, I. M., & Solvang, B. K. (1996). *Metodevalg og metodebruk*. (3. utgave). Oslo: TANO.

Jacobsen, D.I. (2010) *Forståelse, beskrivelse og forklaring.* Høyskoleforlaget.

Johannessen, A., Tufte, P. A., Christoffersen, L. (2010) *Introduksjon til samfunnsvitenskapelig metode.* (4. utgave). Oslo: Abstrakt forlag.

Lindøe, H.P (2018) *Risiko, tillit og kontroll*. Oslo: Gyldendal Norsk Forlag.

Naisbitt, J. (1982). *Megatrends.* Warner Books Inc. New York.

Nasjonal sikkerhetsmyndighet, Politidirektoratet og Politiets sikkerhetstjeneste (2015) *En veiledning i sikrings- og beredskapstiltak mot tilsiktede uønskede handlinger.* Oslo.

NOU 2015: 13. (2015). Digital sårbarhet – sikkert samfunn – beskytte enkeltmennesker og samfunn i en digitalisert verden. Oslo: Justis- og beredskapsdepartementet.

Næringslivets Sikkerhetsråd (2018) Mørketallundersøkelsen 2018. *Informasjonssikkerhet, personvern og datakriminalitet.* Opion AS.

Politiets sikkerhetstjeneste, Nasjonal sikkerhetsmyndighet, Politiet og Næringslivets Sikkerhetsråd (2017) *Sikkerhet ved ansettelsesforhold – før, under og ved avvikling.* Oslo: Kripos

Reason, J. (1997). Managing the Risks of Organizational Accidents. Hampshire: Ashgate Publishing Limited.

Repstad. P. (1993) *Mellom nærhet og distanse: kvalitative metoder i samfunnsfag.* Oslo: Universitetsforlaget

Stranden, R. (2019) *Sikring. En innføring i teori og praksis.* Gyldendal Norsk Forlag AS.

Thagaard, T. (2013). *Systematikk og innlevelse.* 2. Utgave. Bergen: Fagbokforlaget

Tjora, A. (2012). Kvalitative forskningsmetoder i praksis. Oslo: Gyldendal.

Wadel, C. (2014) *Feltarbeid i egen kultur.* Cappelen Dam Akademisk

Westrum, R. (1993) Cultures with requisite imagination, i J.A. Wise, V. Hopkin og P. Stager (red.) *Verification and validation of complex systems. Human factor issues.* Berlin: Springer.

Yin, Robert K. (2014). *Case Study Reserach: Design and Methods*. London: Sage Publications.

8.1 Elektroniske kilder

ATEA (17.10.2018). *Slik bruker hackere ansatte til å få tilgang til selskapets datasystem, og hvorfor bør HR-avdelingen ta et større ansvar?* Hentet fra: https://www.atea.no/siste-nytt/slik-bruker-hackere-ansatte-til-a-fa-tilgang-til-selskapets-datasystem-og-hvorfor-bor-hr-avdelingen-ta-et-storre-ansvar/

CBS News (28.10.2016) *The phishing email that hacked the account of John Podesta.* Hentet fra: https://www.cbsnews.com/news/the-phishing-email-that-hacked-the-account-of-john-podesta/

CISCO (u.å) *What Is Phishing?* Hentet fra: https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html

CISCO (19.10.2018) *Slik bruker hackere ansatte til å få tilgang til selskapets datasystem*. Hentet fra: https://gblogs.cisco.com/no/slik-bruker-hackere-ansatte-til-a-fa-tilgang-til-selskapets-datasystem-og-hvorfor-bor-hr-avdelingen-ta-et-storre-ansvar/

Dagens Næringsliv (26.03.2020) *Oljefondets koronatap: 1330 milliarder kroner.* Hentet fra: https://www.dn.no/marked/oljefondet/koronaviruset/oljefondets-korona-tap-1330-milliarder-kroner/2-1-781858

Digi (26.11.2015) *Advarer mot avansert phishing. Angriperen svarer på norsk.* Hentet fra: https://www.digi.no/artikler/advarer-mot-avansert-phishing-angriperen-svarer-pa-norsk/320202

Digi (24.08.2018) *NotPetya: - Skrinla oppgradering av IT-sikkerheten hos Mærsk fordi det ikke ga lederene økt bonus.* Hentet fra: https://www.digi.no/artikler/notpetya-skrinla-oppgradering-av-it-sikkerheten-hos-maersk-fordi-det-ikke-ga-lederne-okt-bonus/444456

Digi (26.03.2020) *Et digitalt trusselbilde i krisetid.* Hentet fra: https://www.digi.no/artikler/kommentar-et-digitalt-trusselbilde-i-krisetid/488389?fbclid=IwAR3bVhIbHV4SFlh9FahrE0LMVEAV5XT-oNvctO4MhrkUSbL1ZgftdR-vYI0

Digitaliseringsdirektoratet (u.å) *Begrepsliste: Informasjonssikkerhet.* Hentet fra: https://internkontroll-infosikkerhet.difi.no/begrepsliste-informasjonssikkerhet

Eivind Høydal (20.02.2020) *Trusselmodellering i norsk oljesektor.* Hentet fra: https://infosec.sintef.no/informasjonssikkerhet/2020/02/trusselmodellering-i-norsk-oljesektor/

Enerwe (20.03.2016) *22.000 nye oljejobber inne 2020.* Hentet fra: https://enerwe.no/hr-iris-karl-eirik-schjott-pedersen/22-000-nye-oljejobber-innen-2020/131083

Europol (04.11.2019) *Europol publishes law enforcement and industry report on spear phishing.* Hentet fra: https://www.europol.europa.eu/newsroom/news/europol-publishes-law-enforcement-and-industry-report-spear-phishing

E24 (19.03.2019) *Sikkerhetsekspert om Hydro-angrepet: - Dette kan ramme alle, både privatpersoner og virksomheter.* Hentet fra: https://e24.no/teknologi/i/G1odjQ/sikkerhetsekspert-om-hydro-angrep-dette-kan-ramme-alle-baade-privatpersoner-og-virksomheter

Finansavisen (20.03.2020) *Oljeprisen faller videre.* Hentet fra: https://finansavisen.no/nyheter/olje/2020/03/20/7509888/oljeprisen-faller-videre

FuseMail (2017) *Lær organisasjonen å identifisere målrettet phishing*. Hentet fra: https://www.fusemail.com/wp-content/uploads/2017/05/Lær-organisasjonen-å-identifisere-målrettet-phishing_NO.pdf

Hydro (21.08.2019) *Cyberangrep på Hydro.* Hentet fra: https://www.hydro.com/no-NO/media/pa-dagsorden/cyberangrep-pa-hydro/

Kapital (u.å) *Norges 500 største bedrifter.* Hentet fra: https://kapital.no/norges-500-storste

Koordineringsgruppen for IKT-risikobildet. Regjeringen (01.06.2010) *Bakgrunnsnotat. Cybersikkerhet.* Hentet fra: https://www.regjeringen.no/contentassets/252f869fdfac46648e41e6ca5fb0600a/cybersikkerhet_svar-med-merknader_nsm-pst-etterretningstjenesten.pdf

Lysneutvalget (24.04.2015) *Digitale Sårbarheter Olje & Gass.* Hentet fra: https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/sved/5.pdf

Maersk (28.06.2017) *Cyber attack update.* Hentet fra: https://investor.maersk.com/news-releases/news-release-details/cyber-attack-update

Meld. St. 27 (2015-2016) *Digital agenda for Norge. IKT for en enklere hverdag og økt produktivitet.* Hentet fra: https://www.regjeringen.no/contentassets/fe3e34b866034b82b9c623c5cec39823/no/pdfs/stm201520160027000dddpdfs.pdf

Meld. St. 38. (2016-2017) *IKT-sikkerhet.* Hentet fra: https://www.regjeringen.no/contentassets/39c6a2fe89974d0dae95cd5af0808052/no/pdfs/stm201620170038000dddpdfs.pdf

Microsoft (u.å) *Beskytte deg mot phishinangrep og andre typer elektronisk svindel.* Hentet fra: https://support.office.com/nb-no/article/beskytte-deg-mot-phishing-angrep-og-andre-typer-elektronisk-svindel-be0de46a-29cd-4c59-aaaf-136cf177d593?ui=nb-NO&rs=nb-NO&ad=NO

Midsec (17.01.2020) *Kriminaliteten har gått fra gata til data.* Hentet fra: https://midsec.no/2020/01/17/kriminaliteten-har-gatt-fra-gata-til-data/

Nasjonal Sikkerhetsmyndighet (2010) *Rapport om sikkerhetstilstand 2010.* Hentet fra: https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/rst_2010.pdf

Nasjonal Sikkerhetsmyndighet (12.05.2014) *Sikkerhetskultur.* Hentet fra: https://www.nsm.stat.no/om-nsm/tjenester/sikkerhetsstyring/sikkerhetskultur/

Nasjonal Sikkerhetsmyndighet (2015) *Risiko 2015.* Hentet fra: https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2015-web.pdf

Nasjonal Sikkerhetsmyndighet (2016) *Risiko 2016.* Hentet fra: https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2016.pdf

Nasjonal Sikkerhetsmyndighet (2017) *Risiko 2017.* Hentet fra:

https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2017_lr_0404_enkelts_v3.pdf

Nasjonal Sikkerhetsmyndighet (2018) *Risiko 2018.* Hentet fra: https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2018_web.pdf

Nasjonal Sikkerhetsmyndighet (12.03.2019) *Personellsikkerhet.* Hentet fra: https://www.nsm.stat.no/om-nsm/tjenester/personellsikkerhet/

Nasjonal Sikkerhetsmyndighet (2019) *Risiko 2019.* Hentet fra: https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2019_final_enkeltside.pdf

Nasjonal Sikkerhetsmyndighet (17.02.2020) *Løspengevirus.* Hentet fra: https://www.nsm.stat.no/aktuelt/nsm-og-kripos-gir-ut-temarapport-om-losepengevirus/

Nasjonal Sikkerhetsmyndighet (2020) *Risiko 2020.* Hentet fra: https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm-risiko-2020.pdf

Nasjonal Sikkerhetsmyndighet (13.03.2020) *Varsel i forbindelse med koronaviruset.* Hentet fra: https://www.nsm.stat.no/NCSC/ncsc-varsler/ncsc-varsel-i-forbindelse-med-koronaviruset/

Nettvett (03.09.2019) *Phishing.* Hentet fra: https://nettvett.no/phishing/

NHO (30.04.2018) *Hva er et cyberangrep?* Hentet fra: https://arbinn.nho.no/Medlemsfordeler/medlemsfordeler-nho/nho-forsikring2/sporsmal-og-svar/hva-er-et-cyberangrep/

NHO (2018) *Verden og oss – Næringslivets perspektivmelding 2018.*Hentet fra: https://www.nho.no/siteassets/publikasjoner/naringslivets-perspektivmelding/pdf-er-30okt18/nho_perspektivmeldingen_hele_web_lowres.pdf

NorSIS (11.08.2016) *Målrettet phishing-robot på twitter*. Hentet fra: https://norsis.no/malrettet-phishing-robot-pa-twitter/

NorSIS (14.11.2017) *Google studie: hvilken metode er mest effektiv for å kapre en brukerkonto?* Hentet fra: https://norsis.no/google-kapre-brukerkonto/

NorSIS (04.02.2020) *Trusler og trender 2019-2020.* Hentet fra: https://norsis.no/trusler-og-trender-2019-2020/

Norsk olje og gass (18.10.2017) *Olje- og gasshistorien.* Hentet fra: https://www.norskoljeoggass.no/om-oss/oljehistorien/

Norsk olje og gass (April, 2019) *Fakta om norsk olje og gass.* Hentet fra: https://www.norskoljeoggass.no/globalassets/dokumenter/naringspolitikk/fakta-om-norsk-olje-og-gass-april-2019-ver1.pdf

Norsk Petroleum (14.03.2019) *Petroleumsforskning og teknologi.* Hentet fra: https://www.norskpetroleum.no/miljo-og-teknologi/petroleumsforskning-og-teknologi/

Norsk Petroleum (30.01.2020) *Arbeidsplasser.* Hentet fra: https://www.norskpetroleum.no/okonomi/arbeidsplasser/

Norsk Petroleum (07.02.2020) *Statens inntekter.* Hentet fra: https://www.norskpetroleum.no/okonomi/statens-inntekter/

NRK (15.05.2017) *NRKbeta forklarer: dataormen «WannaCry»*. Hentet fra: https://nrkbeta.no/2017/05/15/nrkbeta-forklarer-dataormen-wannacry/

NRK (2020) *Koronaviruset.* Hentet fra: https://www.nrk.no/nyheter/koronaviruset-1.14855584

Petroleumstilsynet (01.01.2011) *§22 Opplæring i sikkerhet og arbeidsmiljø etter arbeidsmiljøloven.* Hentet fra: https://www.ptil.no/regelverk/alle-forskrifter/aktivitetsforskriften/VI/22/

Petroleumstilsynet (26.02.2013) *Kultur og systemer for læring.* Hentet fra: https://www.ptil.no/contentassets/6ab1530ec4a1491b8c224d5d649b5586/kultur-og-systemer-for-laring--en-kunnskapsoversikt-om-organisatorisk-laring-og-sikkerhet.pdf

Petroleumstilsynet (17.04.2019) *Skjerpet innsats for IKT-sikkerhet.* Hentet fra: https://www.ptil.no/fagstoff/utforsk-fagstoff/video/2019/skjerpet-innsats-for-ikt-sikkerhet/

Petroleumstilsynet (17.12.2019) *Klare krav til digitalisering.* Hentet fra: https://www.ptil.no/fagstoff/utforsk-fagstoff/fagartikler/2019/klare-krav-til-digitalisering/

Politiets sikkerhetstjeneste. (2015). *Trusselvurdering 2015*. Hentet fra: https://www.pst.no/globalassets/artikler/trusselvurderinger/trusselvurdering-2015.pdf

Politiets sikkerhetstjeneste. (2016). *Trusselvurdering 2016*. Hentet fra: https://www.pst.no/globalassets/artikler/trusselvurderinger/trusselvurdering-2016.pdf

Politiets sikkerhetstjeneste. (2017). *Trusselvurdering 2017*. Hentet fra: https://www.pst.no/globalassets/artikler/trusselvurderinger/psts-trusselvurdering-2017.pdf

Politiets sikkerhetstjeneste. (2018). *Trusselvurdering 2018*. Hentet fra: https://www.pst.no/trusselvurdering-2018/

Politiets sikkerhetstjeneste. (2019). *Trusselvurdering 2019*. Hentet fra: https://www.pst.no/alle-artikler/trusselvurderinger/trusselvurdering-2019/

Politiets sikkerhetstjeneste. (2020). *Trusselvurdering 2020*. Hentet fra: https://www.pst.no/alle-artikler/trusselvurderinger/nasjonal-trusselvurdering-2020/

Postholm, M.B., (2004) *Kvalitativ forskning på praksis. Fra opprinnelse til forskerfokus.* Hentet fra: https://www.idunn.no/file/pdf/33193666/kvalitativ_forskning_pa_praksis_fra_opprinnelse_til_forskerfokus.pdf

PRO ISP (10.10.2018) *Hvordan avsløre falsk epost og phishing angrep.* Hentet fra: https://www.proisp.no/blogg/hvordan-avslore-falsk-epost/

PwC (28.10.2019) *PwC Cybercrime Survey 2019.* Hentet fra: https://markedsportal.pwc.no/brandportal/pwcportal/public/detail/635?token=9201d6486f907b871d9610317a2208eb

PwC (u.å) *Digitalisering i oljesektoren.* Hentet fra: https://www.pwc.no/no/pwc-aktuelt/digitalisering-i-oljesektoren.html

PwC (u.å) *Digitalisering på 1-2-3.* Hentet fra: https://www.pwc.no/no/teknologi-omstilling/digitalisering-pa-1-2-3.html

Red Level (25.06.2019) *What is spear phishing and how can my company avoid it?* Hentet fra: https://redlevelgroup.com/what-is-spear-phishing-and-how-can-my-company-avoid-it/

Regjeringen (04.09.2018) *Sikkerhet i petroleumsvirksomheten.* Hentet fra: https://www.regjeringen.no/no/tema/arbeidsliv/arbeidsmiljo-og-sikkerhet/innsikt/sikkerhet-i-petroleumsvirksomheten/id568598/

Reuters (06.02.2020) *Saudi Aramco sees increase in attempted cyberattacks.* Hentet fra: https://www.reuters.com/article/us-saudi-aramco-security/saudi-aramco-sees-increase-in-attempted-cyber-attacks-idUSKBN2002N2

SecurityInnovation (u.å) *A Successful Cyberattack Often Starts with the Employee.* Hentet fra: https://web.securityinnovation.com/hubfs/downloads/employee-security-risk.pdf

SINTEF (12.10.2002) *Feiltoleranse, barrierer og sårbarhet.* Hentet fra: https://www.sintef.no/globalassets/upload/teknologi_og_samfunn/sikkerhet-og-palitelighet/rapporter/stf38-a03404.pdf

SINTEF (26.02.2013) *Kultur og systemer for læring.* Hentet fra: https://www.sintef.no/globalassets/upload/teknologi_og_samfunn/sikkerhet-og-palitelighet/sintef-a24120-kultur-og-systemer-for-laring.-en-kunnskapsoversikt-om-

organisatorisk-laring-og-sikkerhet.pdf

SINTEF INFOSEC (30.11.2016) *Sløyfer og slips i ROS analyser.* Hentet fra: https://infosec.sintef.no/informasjonssikkerhet/2016/11/sloyfer-og-slips-i-ros-analyser/

Store Norske Leksikon (27.05.2019) *IKT.* Hentet fra: https://snl.no/IKT

Storebrand (u.å) *Sikkerhet. Råd om hvordan du kan ivareta sikkerheten din på nett.* Hentet fra: https://www.storebrand.no/om-storebrand/sikkerhet-og-personvern/detaljer/

Sysla (30.08.2018) *Tre av fire oljeselskap har vært utsatt for alvorlige dataangrep.* Hentet fra: https://sysla.no/teknologi/a/GGx639/tre-av-fire-oljeselskap-har-vrt-utsatt-for-alvorlige-dataangrep

Teknisk Ukeblad (22.01.2019) *Fersk rapport: Oljebransjen melder om økt rekruttering i 2019.* Hentet fra: https://www.tu.no/artikler/fersk-rapport-oljebransjen-melder-om-okt-rekruttering-i-2019/455954

Trend Micro (2019) *Drilling Deep. A look at cyberattacks on the Oil and Gas Industry.* Hentet fra: https://documents.trendmicro.com/assets/white_papers/wp-drilling-deep-a-look-at-cyberattacks-on-the-oil-and-gas-industry.pdf

Uninett (2013) *Spear Phishing.* Hentet fra: https://www.uninett.no/sites/default/files/webfm/OUCH-201307%20Spear%20phishing.pdf

Vadasecure (19.12.2019) *Why your new employee is a perfect target for a spear phishing attack.* Hentet fra: https://www.vadesecure.com/en/why-your-new-employee-is-a-perfect-target-for-a-spear-phishing-attack/

Wired (22.08.2018) *The Untold Story of NotPetya, the Most Devestating Cyberattack in History.* Hentet fra: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

9.0 Vedlegg

9.1 Intervjuguide

Innledning

1. Hva er din stillingstittel, og hvilke arbeidsoppgaver innebærer den?
a. Hvilken relevant erfaring har du når det kommer til cybersikkerhet?

Cybersikkerhet

2. Hvilke cybertrusler står oljesektoren ovenfor?
a. Eksempler: Phishing, direktørsvindler, DDoS-angrep (tjenestenekt angrep, IoT), honningfeller.

3. Hvilken cybertrussel/metode ser dere absolutt mest av?
a. Hvorfor tror du det skiller det seg ut?

4. Har dere hatt uønskede hendelser relatert til phishingangrep?
a. Ja: Hva bidro til at det skjedde?
b. Nei: Hva bidro til at det ikke skjedde?

5. Hvilken type opplæring gir dere til nyansatte når det kommer til IKT-sikkerhet? Kurs, videoer osv.
a. Ser dere noen effekt av opplæringen? I form av færre uønskede hendelser eksempelvis relatert til phishingangrep.

Ansatte

6. ATEA og Uninett er blant de som trekker frem at phishingangrep mot nyansatte er noe vi bør se opp for i fremtiden. Grunnen er at nyansatte er lite kjent med både folk og prosess i sitt nye arbeidsforhold. I tillegg til at nyansatte ønsker å gi et godt inntrykk og frykter å gjøre feil, dermed kan ønsket om å svare raskt på en e-post gjøre at de blir offer for phishingangrep. I hvilken grad tror dere at nyansatte utgjør en større trussel?

7. Vil du si at sjansen for å bli lurt av et phishingangrep er større for en nyansatt enn en etablert ansatt?
a. Nei: hvorfor ikke?
b. Ja: Hvorfor tror du det?

Kunnskap og kompetanse

8. Norsk senter for informasjonssikring skriver at kunnskap og opplæring kan redusere sjansen for phishingangrep. Hvordan arbeider dere med opplæring for å øke kunnskapen og kompetansen hos de ansatte rundt phishingangrep?

9. Hvordan arbeider dere for å ivareta denne kunnskapen og kompetanse hos de ansatte? Med tanke på oppfølging av den opplæringen de har gått gjennom.

10. Hvordan tror du de ansattes kunnskap og kompetanse påvirker arbeidet med å hindre phishingangrep?

11. Hvordan arbeider dere for å hindre spesifikk phishingangrep? Opplæring, kampanjer, oppfølging, kurs osv.

12. Ser dere noe effekt av arbeidsmetodene dere bruker for å hindre phishingangrep?
a. Hvordan registrere dere denne effekten?

Avsluttende

13. Er det noe ekstra du vil tilføye?

14. Har jeg mulighet til å sende oppfølgingsspørsmål på mail om det er nødvendig?

9.2 Samtykkeerklæring

Jeg studerer master i samfunnssikkerhet ved Universitetet i Stavanger. Masteroppgaven min omhandler phishingangrep i oljesektoren. I den forbindelse ønsker jeg å intervjue ansatte i oljeselskaper. Spørsmålene vil omhandle deg og din bakgrunn, cybertrusler, phishingangrep m.m.

Oppgaven vil bli publisert på internett, av den grunn anonymiseres alle selskaper og informanter i oppgaven. Jeg ønsker å ta opptak av samtalen for å skape en bedre dialog under selve intervjuet. Opptaket blir slettet så fort intervjuet er transkribert. Masteroppgaven skal etter planen leveres 15.06.2020, da vil også alle notater fra intervjuene bli slettet.

Det er frivillig å delta i studien, og du kan når som helst trekke ditt samtykke uten å oppgi noen grunn. Dersom det er ønskelig kan jeg også sende intervjuet til deg for godkjenning før det legges inn i oppgaven.

Samtykke
Jeg har mottatt informasjon om studien, og er villig til å delta:

(Signatur informant, sted og dato)