DET TEKNISK-NATURVITENSKAPELIGE FAKULTETET

MASTEROPPGAVE

Studieprogram/spesialisering:	**Vårsemesteret, 2023**
Samfunnssikkerhet	Åpen oppgave
Forfatter:	
Elisabeth Risa	
Fagansvarlig ved UiS:	
Førsteamanuensis Morten Sommer	
Tittel på oppgaven:	
På innsiden av løsepengevirusene: *En analyse av ofrenes betalingsbeslutninger:* *De som ikke betalte.*	
Studiepoeng:	
30	
Emneord: Risiko, risikovurdering, dataangrep, løsepengevirus, løsepenger, kost-nytteanalyse, krise, krisehåndtering, trussel, betalingskrav, beslutningstaking, usikkerhet	**Sidetall + vedlegg:** 94 + 1 = 95 Stavanger, 15. juni 2023

Forord

Høsten 2021 sitter jeg i vinduskarmen på Ostehuset Hinna med pensumartikler og datamaskin. Utenfor glassvinduet vrimler det av små og store som skal på Viking-kamp på SR-Bank Arena tvers over gaten. Kafeen er full av besøkende, like ved siden av meg sitter en mann som skal på fotballkamp.

Han spør: - *Hva leser du?*
Jeg svarer at jeg leser om samfunnssikkerhet, om hvordan vi forsterker samfunnet slik at vi på best mulig vis unngår uønskede hendelser.

Det er da han forteller meg at han er daglig leder for en mellomstor bedrift i Jåttåvågen, og at virksomheten hans nylig var utsatt for et dataangrep.

- *Vi kom på jobb. Alle dataskjermene var svarte. Den eneste skjermen som lyste i lokalet viste et digitalt trusselbrev som forklarte at vi måtte betale for å få igjen tilgangen til våre data.*

Han sukker tungt når han forteller.

Jeg spør: - *Hva gjorde dere?*

Han ser ut av vinduet, før han svarer: - *Vi ringte politiet. Damen i andre enden sa hun skulle sende en patrulje.*

Han sukker igjen. Raskt forklarer han at saken ble aldri løst med politietterforskning hvor angriperne ble dømt og straffet.

- Vi betalte pengekravet og kontaktet et IT-firma som forsterket brannmurer og tettet «hullene» i systemet. Alternativet var konkurs. Alt vi hadde av verdi var lagret i datafilene angriperne hadde kryptert.

Denne oppgaven er dedikert til mannen i vinduet som delte historien om løsepengeviruset.

Målet med oppgaven er å identifisere suksessfaktorene til fem virksomheter, alle utsatt for tilsvarende løsepengevirus som mannen i vinduet, men hvor angrepet ble løst uten å betale pengekravet.

Håpet er at en systematisk gjennomgang av andres suksesshistorier kan bidra til å vise vei for andre virksomheter som havner i tilsvarende vanskelige og umulige situasjon som mannen i vinduet. For hans historie er ikke unik.

Elisabeth Risa
Stavanger, 15. juni 2023

Sammendrag

Det europeiske byrået for nettverks- og informasjonssikkerhet, ENISA, har siden 2021 rangert løsepengevirus som den største digitale trusselen over hele EU. Samme byrå anslår at over seksti prosent av de berørte virksomhetene ga etter for truslene og betalte store penger til kriminelle hackere for å få data tilbake etter å ha blitt utsatt for et løsepengevirus.

Løsepengevirus er når kriminelle hackere kommer på innsiden av en virksomhets datasystem, låser systemene og krever penger for å låse opp. Løsepengevirusene anses som et komplekst fenomen som involverer to typer kriminalitet, først hacking og deretter pengeutpressing. Også i Norge byr løsepengevirusene på utfordringer, både for privat og offentlig virksomhet. En av årsakene til at den digitale utpressingen øker er fordi mange betaler. Det har gjort løsepengevirusene til en lukrativ virksomhet for datakriminelle.

I denne komparative casestudien har målet vært å undersøke hvilke faktorer som til sammen bidro til en suksessfull håndtering av selve betalingskravet et løsepengevirus medfører. Sagt på en forenklet måte: Hva hadde de til felles - de som ikke betalte?

Studien dokumenterer at sammenfallende faktorer var å ta saken på alvor, etablere krisestab, ha ledelsens fulle støtte, beslutte under usikkerhet og forsøke å etablere en tidslinje for når angrepet skjedde, sistnevnte var for å finne ut hvor lenge angriperne hadde vært inne i systemet. En annen faktor som inngikk i beslutningsunderlaget var å ikke ville støtte kriminelle bakmenn og at betaling ikke ville medføre garanti for å få data i retur. Ikke i noen av sakene ble det opprettet kontakt med angriperne. Det ble i stedet hentet inn støtte fra eksterne. Til slutt var det avgjørende at menneskene støttet og motiverte hverandre.

Disse ni faktorene var til stede hos alle de undersøkte casene, og bidro til at virksomhetene ikke betalte. Funnenes overføringsverdi inngår som en egen del i drøftingen og viser at en ren kost-nytte analyse er et for snevert beslutningsgrunnlag. Datagrunnlaget for studien er kvalitativ, men inkluderer en dokumentanalyse for å styrke oppgavens reliabilitet.

Begreper

Krise: «En alvorlig trussel mot strukturer, verdier og normer i et sosialt system som under tidspress og usikkerhet gjør det nødvendig å foreta kritiske beslutninger» (Rosenthal, Charles & t´Hart, 1989, s. 10).

Risiko: «Refererer til usikkerheten om og alvorligheten av hendelser og konsekvenser (eller resultater) av en aktivitet med hensyn til det mennesker verdsetter» (Aven & Renn, 2010, s.3).

Risikovurdering: Samlet prosess som består av planlegging, risikoanalyse og risikoevaluering (Rausand & Utne, 2009, s. 90).

Trussel: Kan være hva som helst, enten fysisk eller abstrakt, dersom det har potensialet til å negativt påvirke et objekt eller system (Bergsjø et al., 2020, s. 147).

Sårbarhet: «Et uttrykk for de problemer et system får med å fungere når det utsettes for en uønsket hendelse, samt de problemer systemet får med å gjenoppta sin virksomhet etter at hendelsen har inntruffet». (NOU 2000 s. 24. Et sårbart samfunn – Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet).

Beredskap: Alle tekniske, operasjonelle og organisatoriske tiltak som hindrer at en inntrådt faresituasjon utvikler seg til en ulykkessituasjon, eller som hindrer eller reduserer skadevirkningene av inntrådte ulykkessituasjoner (Aven et al., 2004, s. 121).

Krisehåndtering: Den umiddelbare og påfølgende responsen, forberedt eller ad-hoc, når en krise har manifestert seg (Engen et al., 2016, s. 342).

Kritisk infrastruktur: Anlegg og systemer som er helt nødvendige for å opprettholde samfunnets kritiske funksjoner (NOU 2015: 13, s. 19).

Kryptere data: En matematisk metode som sørger for at data blir utilgjengelige ved at de ikke er lesbare. Informasjonen «låses ned» med en nøkkel og kan ikke leses før man har låst den opp igjen med riktig nøkkel. (Datatilsynet, 2012).

Dekryptere data: Prosessen som gjør data lesbare igjen. (Datatilsynet, 2012).

Krypteringsnøkkel: En tilfeldig streng med tegn som er opprettet eksplisitt for kryptering og dekryptering av data. (Telenor).

Løsepengevirus/Ransomware: Skadevare som benyttes av en angriper med et bestemt formål om å hindre virksomheten i å bruke sitt eget IT-system, slik at virksomheten presses til å betale for å komme seg ut av situasjonen. Det gjøres ved å enten låse/kryptere tilgangen til virksomhetens filer eller ved å låse/sperre pålogging til en bestemt maskin eller tjeneste. Det kan også komme trusler om å publisere virksomhetens sensitive dokumenter og annen data hvis ikke virksomheten betaler. Merk at løsepengevirus sjeldent er virus-basert, tross for begrepet. (NSM: Sikkerhetstiltak mot digital utpressing og andre angrep).

Tingenes internett: På engelsk forkortet til IoT (Internet of Things) gjengis som et samlebegrep om hvordan internett benyttes «for å koble sammen stadig flere autonome komponenter til et komplekst system». Alt som kobles til internett kan kommunisere med hverandre og slik deles informasjon fra innebygde sensorer (NOU, 2015, s. 13 og s. 46).

«**Shaminglist»:** Taktikk for å presse ofre til å betale mer, raskere eller begge deler. En dobbel utpressing teknikk: Uteblir betaling truer angriper både med å offentliggjøre angrepet på en slags «wall of shame»-liste på det mørke nettet samt å selge stjålne dataene videre til andre (Securityworldmarket, 2020).

Hacker: I dagligtale har dette blitt synonymt med en som finner løsninger og snarveier for å komme på innsiden av datasystemer og nettverk (Telenor).

Forkortelser

ARPA The Advanced Research Projects Agency

CERT Computer Emergency Response Team

CSIRT Computer Security Incident Response Team

CTA The Cyber Threat Alliance

DSB Direktoratet for Samfunnssikkerhet og Beredskap

ENISA The European Union Agency for Cybersecurity

GDPR General Data Protection Regulation

IKT Informasjons- og kommunikasjonsteknologi

KRIPOS Nasjonal enhet for bekjempelse av organisert og alvorlig kriminalitet

NCSC National Cyber Security Centre

NOU Norges Offentlige Utredninger

NORSIS Norsk senter for informasjonssikring

NSM Nasjonal sikkerhetsmyndighet

NSR Næringslivets sikkerhetsråd

Figurer og tabeller

INNHOLDSFORTEGNELSE

1.0 Introduksjon

Før var virksomheter med kassebeholdning utsatt for ran. Kriminelle trengte seg inn med våpen for å true til seg penger. Nå hører fysiske ran til sjeldenhetene. I stedet er metodene digitale. Kriminelle gjør digitale innbrudd, stjeler data og truer med publisering og videresalg om de ikke mottar betaling. Det er dette som er løsepengevirusene, omtalt av ENISA som den største digitale trusselen over hele EU siden 2021. Mye av årsaken til at løsepengevirusene øker er fordi de fleste betaler.

Til tross for at løsepengevirusene får mye oppmerksomhet, finnes det lite forskning om betalingsdilemmaet angrepene medfører. Tema for denne oppgaven er å undersøke hva fem virksomheter gjorde da de var angrepet av løsepengevirus, skjermene var svarte og kritiske beslutninger måtte tas. Siden det ikke finnes særlig nasjonal forskning på området (se neste kapittel) er det jobbet med å forsterke oppgavens indre validitet slik at funnene kan ha overføringsverdi for andre som kommer i samme situasjon i fremtiden.

1.1 Tidligere forskning

I dette delkapittelet undersøkes og redegjøres det for hvilken forskning som allerede finnes om betalingsbeslutninger og løsepengevirus i Norge. Formålet er å etablere en oversikt over hva som er eksisterende kunnskapsstatus og sette min forskning inn i en større sammenheng.

Forskningsfeltet innen datakriminalitet er stort. Tidlig på våren 2023 ga et søk på søkeordet `ransomware` i Google Scholar et resultat på 44.000 treff. Det vil være en for stor jobb å sette seg inn i alle artiklene, men mer målrettede søk i databasen på «ransomware» og «payment» ga 23.000 treff og ved å gå gjennom de første ti-talls sidene varierer treffene fra detaljerte artikler om etiske betraktninger om å betale - eller ikke betale, hvordan problemet kan unngås samt studier om betalingsbeslutninger – både for virksomheter som har betalt og ikke betalt. Det kommer senere i denne oppgaven en nærmere omtale av noen av de mest relevante studiene om dette, det er gjort for å sette min forskning inn i en bredere kontekst og for å tilføre relevante drøftingsmoment.

Samtidig har jeg gjort tilsvarende søk i anerkjente norske fagdatabaser og portaler for masteroppgaver og doktorgradsavhandlinger. På Munin (Norges Arktiske Universitet) gir et

søk på ‘løsepengevirus’ tre treff, Brage, Universitetet i Stavanger sitt åpne digitale arkiv for vitenskapelige publikasjoner, gir femten treff. Søk på 'løsepengevirus' ved Universitetet i Bergen (UiB, BORA) avstedkommer to treff, søk etter løsepengevirus og betaling gir ingen resultat. Søk på løsepengevirus i DUO (UiO) gir null treff, men når jeg legger til «betaling» gir dette 219 treff. En systematisk gjennomgang avdekker en relevant masteroppgave fra Institutt for kriminologi og rettssosiologi ved det juridiske fakultet i Oslo. Oppgaven handler om løsepengevirusangrep mot norske virksomheter. Her er det skrevet noe om betaling i forbindelse med angrep, men hovedformålet er å undersøke politiets forebyggende og konsekvensreduserende rolle ved slike hendelser samt å analysere dynamikken mellom det offentlige og private sikkerhetstilbudet. I samme oppgave poengteres det at løsepengevirus er understudert i Norge hvor det trengs mer forskning (Østbø Lorentzen, 2021, s. 5).

Jeg går dermed videre med å etablere en tydeligere kontekst for denne studien. Først beskriver jeg hva internett er og setter digital vekst inn i en samfunnssikkerhetskontekst. Deretter utvides kapittelet med å beskrive datakriminalitet sammen med et historisk bakteppe for hvordan kriminaliteten inntok den digitale sfæren. Derpå beskrives løsepengevirus og det mørke nettet. Til slutt gis et kort omriss av mørketallproblematikken innen datakriminalitet. Dette gjøres for å skape forståelse for at temaet datakriminalitet fortsatt er ungt og dynamisk, det er mye som skjer på nettet som holdes skjult, det er mye vi ikke vet - eller kan vite - da den digitale utviklingen skjer raskt. Poenget med et slikt bakteppe er å vise den «røde tråden» fra «alt» startet i 1969 og frem til i dag.

1.2 Kontekst: Fremveksten av internett, dataangrep og løsepengevirus

Det finnes flere beretninger om hvordan internett startet. I en del av litteraturen vises det til at internett kom til verden i 1969 da fire datamaskiner, alle «knyttet» sammen i et nettverk, var startskuddet. Hendelsen refererer til etaten ARPANET (The Advanced Research Projects Agency) i det amerikanske forsvarsdepartementet som hadde ansvar for å utvikle ny teknologi for militæret (Hauben, 2007). Fra der skjedde ting fort, på midten av 1990-tallet begynte internett for «alvor» å bli allemannseie, spesielt i den vestlige industrialiserte verden (Yar & Steinmetz, 2019, s. 3). Med dette som bakgrunn ble internett et raskt voksende fenomen som også introduserte nye sårbarheter og risikoer (Renaud et al., 2020). Yar og Steinmetz (2019) viser til at kriminalitet i den digitale sfæren etablerte seg og at utviklingen må sees i sammenheng med fremveksten av internett (Yar & Steinmetz, 2019).

Begrepet "Tingenes internett", på engelsk kalt Internet of Things (IoT), gjengis som et samlebegrep som handler om hvordan internett benyttes «for å koble sammen stadig flere autonome komponenter til et komplekst system» (NOU 2015: 13 s. 46). Alt som kobles til internett kan kommunisere med hverandre og på den måten deles informasjon fra innebygde sensorer (ibid). Direktoratet for samfunnssikkerhet og beredskap (DSB) publiserte i 2020 rapporten *Risikostyring i digitale verdikjeder.* Her peker de spesielt på sårbarhetene alle de direkte koblingene mellom datamaskiner medfører: «De digitale verdikjedene er komplekse, lite oversiktlige, tett koblede og i stor grad transnasjonale. En feil et sted i kjeden kan medføre momentan svikt i viktige tjenesteleveranser et helt annet sted» (Risikostyring i digitale verdikjeder, 2020, s. 3). Med dette som bakteppe går jeg videre til å beskrive hva et løsepengevirus er.

1.3 Løsepengevirus - hva er det?

Løsepengevirus. Ransomware. Utpressingsvare. Cyberutpressing. Gisselvare. Utpressingsprogramvare. Masseutpressing. I dagligtalen, i norske medier og i offentlige publikasjoner brukes mange ulike ord. Det gjelder også i den akademiske litteraturen, et søk på Google Scholar gir treff på de fleste ordene som er listet opp over. Det er derfor nødvendig for meg å klart avgrense og definere hva som menes i den videre omtalen av `løsepengevirus`. For å legge en klar definisjon til grunn ser jeg til CTA (Cyber Threat Alliance), en ideell organisasjon som jobber for å forbedre cybersikkerheten til det globale digitale økosystemet ved å muliggjøre deling av informasjon om cybertrusler mellom selskaper og organisasjoner på cybersikkerhet-feltet. CTA publiserte i 2015 rapport hvor de introduserte følgende definisjon som beskriver denne studiens hovedtema:

«Ransomware er en type skadelig programvare som krypterer et offers filer og deretter krever betaling i retur for nøkkelen som kan dekryptere nevnte filer. Når løsepengevare først installeres på et offers maskin vil det vanligvis målrette seg mot sensitive filer som for eksempel viktige økonomiske data, forretningsdokumenter, databaser, personlige filer mm» (Cyber Threat Alliance, 2015, s. 2). Videre i oppgaven er det denne definisjonen som danner grunnlaget for hva et løsepengevirus er.

1.4 Datakriminalitet og løsepengevirus

I den digitale verden anses datakriminalitet som en stadig større trussel (Europol, 2021). I 1996 publiserte forskerne Young og Yung artikkelen `Cryptovirology: Extortion-Based Security Threats and Countermeasures´ (1996), denne omtales som den første akademiske artikkelen som beskrev hvordan datavirus kunne brukes som verktøy for både utpressing og kriminell aktivitet (Young og Yung, 1996, s. 2). Siden den gang har den kriminelle, digitale aktiviteten ekspandert. Alt fra innbyggere, virksomheter, organisasjoner og stater opplever ondsinnede angrep på informasjonssikkerheten i form av phishing, skadelig programvare, ondsinnede statsaktører og handlinger fra andre motiverte og ressurssterke individer som forsøker å stjele, ødelegge og bedra (Xavier & Pati, 2012, Nichols, 2019 og Renaud mfl., 2020).

Det europeiske byrået for nettverks- og informasjonssikkerhet, ENISA, har siden 2021 rangert trusselen om løsepengevirus øverst i byråets årlige trusselvurderinger. ENISA-rapporten «*Threat Landscape for Ransomware Attacks»* omtaler løsepengevirus som den største trusselen innenfor det digitale formatet over hele EU. «Motivert hovedsakelig av grådighet etter penger, løsepengevare- forretningsmodellen har vokst eksponentielt det siste tiåret». (ENISA, 2022, s. 7) I samme rapport vises det til at metoden for utpressing bare i 2025 vil koste mer enn ti billioner dollar, beløpet tilsvarer nær halvparten av det norske statsbudsjettets samlede inntekter (Statsbudsjettet 2023: Statens inntekter og utgifter). Seks av ti europeiske bedrifter som ble rammet av løsepengevirus i 2020 betalte angriperens pengekrav. Andelen angrep med løsepengevirus økte med 63 prosent i Europa i 2022 (ibid).

1.5 Løsepengevirus i Norge - hva vet vi

Nasjonal sikkerhetsmyndighet (NSM) publiserte i 2021 rapporten «Nasjonalt *digitalt Risikobilde 2021»* som omhandler det nasjonale, digitale risikobildet. Rapporten viser at digital utpressing, med krav om løsepenger, fortsetter å øke i både omfang og antall. Konsekvensene har ført til flere tilfeller av store systemlammelser. Resultatet har vært utilgjengeliggjøring av funksjoner, varer og tjenester. Sensitiv informasjon har kommet på avveie. Det neste sitatet, hentet fra rapporten, beskriver hva som skjer når data krypteres og hvordan dette fører til pengeutpressingen:

«Ved kryptering krever aktøren løsepenger for å dekryptere virksomhetens systemer, og ved publisering kan aktøren true virksomheten med å publisere data som er hentet ut fra virksomheten» (NSM, 2021, s. 20). Nasjonalt cybersikkerhetssenter (NCSC) observerte bare fra 2019 til 2021 en tredobling av alvorlige hendelser i det digitale rom knyttet til krypteringsvirus og økonomisk motivert kriminalitet på nett (NSM, 2021, s. 5).

1.6 Det mørke nettet

Gabriel Weimann, professor i kommunikasjon Haifa-universitetet i Israel, har over flere tiår sporet og undersøkt terroristaktiviteter på nettet. I artikkelen «The Dark Web» fra 2016 definerte Weimann det mørke nettet som «den delen av nettet som inneholder generelt ulovlig og antisosial informasjon, og som kun kan nås gjennom spesialiserte nettlesere» (Weimann, 2016, s. 196). Weimann oppsummerer: «Dark Web brukes til materiale som barnepornografi, uautoriserte lekkasjer av sensitiv informasjon, hvitvasking av penger, brudd på opphavsrett, kredittkortsvindel, identitetstyveri, ulovlig salg av våpen og så videre» (ibid). I denne mørke delen av internett har terrorfinansiering fått fotfeste ved at også terroristenes metoder er blitt digitale (ibid).

Sikkerhetsselskapet Trend Micro publiserte i 2020 en rapport som beskriver hvordan «omsetningen» av stjålne data skjer på det mørke nettet, her tilgjengeliggjøres stjålen data slik at cyberkriminelle kan gjennomføre enda mer effektive dataangrep for så å omsette dataen til aktører som vil utrette mer målrettet skade. Dette er relevant for denne oppgaven fordi det åpner horisonten for hvor skadelig et angrep kan være: «Problemet» er langt fra over eller løst selv om man ikke betaler. De stjålne dataene kan utnyttes av andre ondsinnede aktører til å gjøre mer skade. I dette mørke universet får den stjålne daten en ytterligere verdi som ifølge Trend Micro-rapporten varierer fra et par hundre dollar til flere tusen dollar. Ved å sette opp fremgangsmåten i en modell synliggjøres sårbarhetene gjennom flere ledd:

1. **Virksomhet utsatt for dataangrep:**

→ Trussel om betaling for å få igjen stjålne data

2. **Uteblir betaling:**

→ Ny trussel: Stjålne data «omsettes» ellers publiseres på det mørke nettet

3. **Konsekvens:**

→ Offer utsettes for enda større sårbarheter.

Som vi ser kan veien fra det å komme på jobb når alle dataskjermer er svarte, datatilganger er kryptert og virksomheten utsatt for løsepengevirus, ikke bare bety håndtering av et pengekrav. En risikerer også at virksomhetens eiendeler, de stjålne dataene, misbrukes ytterligere av andre ondsinnede aktører som kan ha helt andre intensjoner enn «bare» å drive med direkte pengeutpressing.

1.7 Formål og problemstilling

Formålet med studien er å identifisere hvilke faktorer som bidro til at fem virksomheter, både private og offentlige, løste betalingskravet løsepengevirusene medfører - **uten** å betale. Connolly og Borrion (2022) viser til at «Ransomware er et komplekst fenomen som involverer to typer kriminalitet: hacking og cyberutpressing. Begge forbrytelsene må være vellykket for at lovbrytere skal høste en økonomisk belønning» (Connolly & Borrion, 2022, s. 2). En virksomhet som utsettes for løsepengevirus må løse flere problemer for å komme tilbake til normalen. Rent teknisk må det også settes av ressurser for å løse de datatekniske utfordringene et hackerangrep medfører. Det er ikke den delen av et løsepengevirus denne studien undersøker. Denne studien ser på fenomenet og effekten av `cyberutpressing` eller ´digital utpressing´ hvor ofrene gjennom et trusselbrev kreves for penger. Trusselbrevet beskriver skadeomfanget, krav om løsepenger og konsekvensene av å ikke betale..

Problemstillingen som har vært førende er slik: **Hvilke faktorer bidro til en suksessfull håndtering av betalingskravet et løsepengevirus medfører?**

For å svare på problemstillingen gjennomføres det kvalitative intervju med fem informanter. Alle var en del av beslutningsgruppen da virksomheten løste angrepet og alle informantene har samtykket til identifisering og dele åpent av sine erfaringer. At håndteringen endte som en suksesshistorie handler om at det ikke ble utbetalt løsepenger slik angriperne krevde. I den forstand foreligger det en objektiv vurdering av at det å ikke betale er brukt som indikatorer for suksess. Collins og Baccarini (2004) understreker at «Det er viktig å skille mellom suksesskriterier og suksessfaktorer. Kriterier brukes for å måle suksess, mens faktorer gjør det lettere å oppnå suksess» (Collins & Baccarini, 2004, s. 3). Faktorer forklares da som hendelser eller årsaker som førte til suksess (ibid). Problemstillingen anses å være relevant for andre virksomheter som vil møte tilsvarende utfordringer i fremtiden. Studien har ingen forskningsspørsmål. Argumentene for det er slik: Hadde betaling av løsepengevirus vært et

tema det var forsket på mye fra før kunne forskningsspørsmålene tilført en nyttig hensikt og spisset forskningen mot ny kunnskap, men i denne studien undersøker et tema som i Norge knapt er kartlagt før og slik jeg ser det kunne forskningsspørsmål bidratt til å begrense eller styre det jeg helt åpent ville undersøke og slik kunne en gått glipp av vesentlige momenter jeg på forhånd ikke så. I resten av dette delkapittelet presenteres kort hvilke avgrensninger som er gjort med en påfølgende oversikt over hvordan oppgaven er strukturert.

1.8 Avgrensning

Oppgaven er skrevet ved Det teknisk-naturvitenskapelige fakultetet ved UiS og er en del av masterutdanningen innen samfunnssikkerhet. Omfanget av oppgaven er 30 studiepoeng som gjennomføres i løpet av tjue uker våren 2023. Problemstillingene begrenses til å besvares gjennom en komparativ casestudie supplert med en dokumentanalyse. Antall caser er satt til fem, dette er på grunn av tidsperspektivet for oppgaven. Casene er valgt for å representere en bredde i det norske arbeidslivet. Studien undersøker virksomhetenes betalingsbeslutninger relaterte til et løsepengevirus. Bakgrunnen er en rekke rapporter fra ENISA, EU og NSM omtaler det er et stort problem at mange betaler når de utsettes for løsepengevirus.

1.9 Oppgavestruktur

Studien inneholder sju hovedkapitler. Kapittel en starter med innledning for tema og setter studien inn i en samfunnssikkerhetskontekst sammen med problemstilling. Kapittel to er teori. Kapittel tre handler om metodevalg. I kapittel fire presenteres empiri, kapittel fem utgjør oppgavens drøftingskapittel for å besvare problemstilling. Kapittel seks byr på anbefaling for videre forskning og konklusjon. Oppgavens struktur ser slik ut:

1. Innledning, kontekst og problemstilling →
2. Teori →
3. Metode →
4. Empiri →
5. Drøfting →
6. Konklusjon

2.0 Teori

I teoridelen er målet å presentere teori som skal bidra til å besvare oppgavens problemstilling. Problemstillingen handler om å identifisere suksessfaktorer for å kunne håndtere betalingskravet et løsepengevirus medfører. Teoridelen er delt inn i fire hovedbolker:

Del én handler om risiko, det er tatt med fordi problemstillingen handler om et løsepengevirus som i seg selv er en risikofylt hendelse, målet er å beskrive hva risiko er og hvordan mennesker forholder seg til risiko. Her er også et overordnet rammeverk for risikostyring tatt med, det er for å se på løsepengevirus i et helhetlig perspektiv.

Del to handler om krise. Teorier om krise er inkludert fordi problemstillingen som skal undersøkes handler om en kritisk situasjon og for at en gjennom besvarelsen av problemstillingen kritisk skal undersøke om, hvordan og på hvilken måte angrepene og løsepengevirusene faktisk utgjorde en krise.

Del tre er teorier om krisehåndtering og beslutninger. Problemstillingen for oppgaven handler om et betalingskrav, det betyr at virksomhetene måtte håndtere og fatte beslutninger i saken om løsepengevirus.

Den fjerde delen handler om pengepolitikk, det er tatt med fordi å kunne besvare problemstillingen må en ha på plass de ytre rammene; er det for eksempel lovstridig i Norge å betale løsepenger? Teoribidragene skal på denne måten til sammen brukes for å drøfte oppgavens problemstilling.

2.1 Risiko

Dette kapittelet skal skape en forståelse for hva risiko er og teoretisk beskrive elementene risiko, usikkerhet og frykt. Grunnen til å velge teori om risiko er at et løsepengevirus kan sette virksomheter fullstendig ut av normal drift, for å løse en slik situasjon må ofrene forholde seg til risiko. Å se på ulike sider av risiko vil bidra til å belyse problemstillingen som handler om virksomhetens betalingsbeslutninger. Det trekkes også inn et rammeverk for helhetlig risikostyring, det er for å belyse oppgavens problemstilling som senere skal drøftes på et overordnet nivå.

2.1.1 Hva er risiko?

Det finnes ingen entydig svar på hva risiko er. I sin enkleste form kan risiko forstås som en kombinasjon av usikkerhet og konsekvenser av en aktivitet. Ved å kvantifisere risiko predikeres eller estimeres sannsynligheten for fremtiden og konsekvensene av disse, og risiko blir et rent produkt av sannsynlighet og konsekvens. I konteksten av løsepengevirusene kunne en slik regnet ut hvor mange løsepengevirus virksomheten har opplevd over et antall år, og funnet sannsynligheten for at det kunne skje. Spørsmålet er om en slik «måling» er nok?

Risiko kommer i mange former. Risiko, etter dagens syn, strekker seg utover det tallmessige og tar innover seg hvordan risiko blir oppfattet og forstått. Aven og Renn (2010) definerer det på denne måten: «Risiko refererer til usikkerheten om og alvorligheten av hendelser og konsekvenser av en aktivitet med hensyn til det mennesker verdsetter» (Aven & Renn, 2010, s. 3).

Definisjonen skiller seg fra den tradisjonelle dimensjonen risiko = sannsynlighet x konsekvens på flere måter. Først refererer definisjonen til at risiko er usikkerheten om hendelser eller konsekvenser av en aktivitet sett i relasjon til alvorligheten. Alvorlighet henviser videre til størrelsen eller omfanget i forhold til noe mennesker verdsetter. Hva mennesket verdsetter er individuelt. Det som kan være verdifullt for den ene, kan være av liten eller ingen verdi for andre. Dette kommer jeg tilbake til senere i oppgaven. Men først er det viktig å slå fast at for denne oppgaven er det Aven og Renn (2010) sin definisjon som legges til grunn. I kontekst til denne studien representerer et løsepengevirus en situasjon med høy grad av usikkerhet, konsekvensene er usikre og det følger av løsepengeviruset at det oppstår verditap - som er viktige på mange måter - for menneskene som er berørt.

For å dykke videre ned i risikobegrepet, hva det er og hva som beskriver dagens «risikosamfunn» beskriver den tyske sosiologen Ulrich Beck (1997) hvordan alt vi omgir oss med handler om samspillet mellom komplisert teknologi og hvordan komplekse og sammensatte organisasjoner og individuell handling stadig endrer seg. Samtidig, beskriver Beck, blir det mer avhengighet på tvers av virksomheter og geografiske områder:

«Risikoer går på tvers av skillet mellom teori og praksis, på tvers av fag- og disiplingrenser, på tvers av spesialisert kompetanse og institusjonelle ansvarsområder, på tvers av skillet

mellom verdier og kjensgjerninger (…) og på tvers av de tilsynelatende institusjonelt atskilte områdene politikk, offentlighet, vitenskap og økonomi» (Beck, 1997, s. 89).

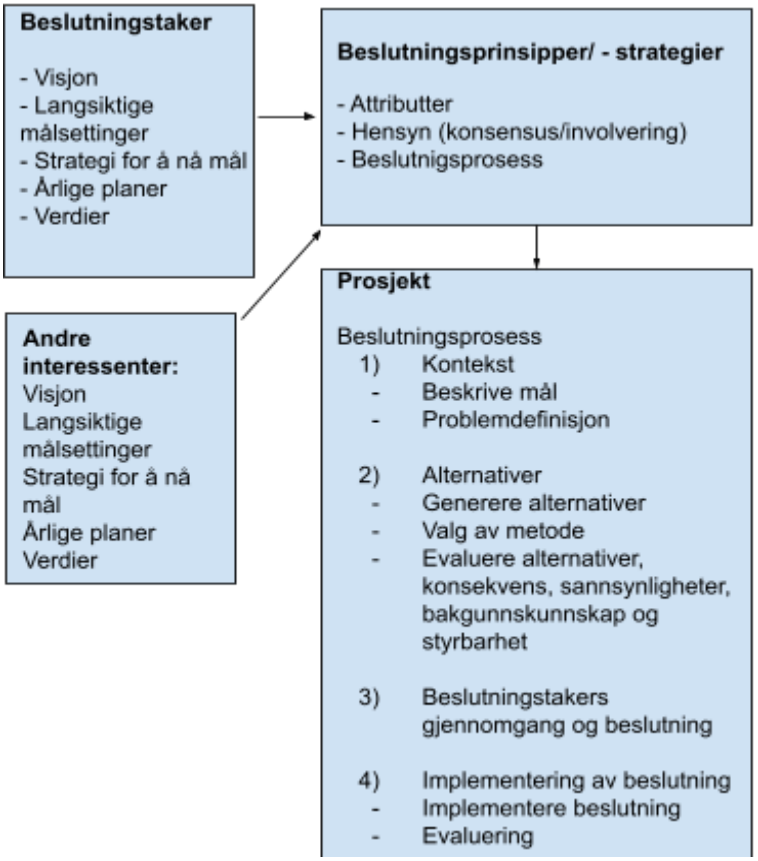
Beck (1997) beskriver hvordan samspillet har bidratt til fremdrift, utvikling, produktivitet og effektivitet, men at de tette koblingene medfører økt sårbarhet og større konsekvenser om en uønsket hendelse inntreffer (ibid). Overført til denne studien er *samspillet* relevant. Samspillet mellom mennesker, teknologi (data) og digitalisering er tett koplet på den måten at rammes et datasystem, vil det oppleves som en stor belastning. Både for et konsern med flere tusen ansatte - eller et enkeltindivid. Det tar oss videre til hvordan menneskene individuelt oppfatter risiko. Det handler om den enkeltes risikoforståelse og risikopersepsjon.

Med risikopersepsjon menes; «Hvordan folk flest forstår, opplever og håndterer risiko og farer» (Aven et al., 2004 s. 40). Et eksempel er om en skal over en trafikkert veg eller krysse en glatt brygge. Da må en gjøre vurderinger for hvor, når og hvordan det skal gjøres på tryggest måte. En må også vurdere konsekvensene valget medfører. Oppstår en uønsket hendelse, om en blir påkjørt eller faller på brygga, vil den enkeltes forståelse og oppfatning av risiko ha innvirkning for håndteringen. En person vurderer det er trygt å krysse bryggen, om en faller er sykehuset innen rekkevidde og en nabo vil ringe ambulanse. En annen vil unngå å krysse brygga fordi et tilsvarende tidligere fall medførte et krevende beinbrudd. Nøyaktig hvordan individer responderer på risiko avhenger av deres oppfatning av risiko, ifølge Renn (2008). Selv om flere individer står overfor den samme risikoen, vil den enkelte oppfatte situasjonen ulikt og derav reagere forskjellig på risiko (ibid). Opplevelsen av risiko er både individuell og subjektiv. Hva noen mennesker ser på som risiko trenger ikke nødvendigvis å bli sett på som risiko av andre. Men hvordan skal virksomheter styre risikoen på sine arbeidsplasser?

2.1.2 Et rammeverk for risikostyring

Terje Aven (2015) foreslår et rammeverk for risikostyring (Aven, 2015, s. 146 - 147). I modellen inngår flere elementer som til sammen utgjør en overordnet risikotenkning dersom kunnskapen er svak og usikkerheten stor. Aven (2015) skriver at risikostyring er ikke en ubalansert eller ensidig prosess for risikoreduksjon i samfunnet, det handler om balansen mellom å unngå skader, ulykker og tap på den ene siden, på motsatt side handler det om utvikling og verdiskapning (Aven, 2015). For å beskrive deltakerne i Avens modell kan

beslutningstakere være en person, et styre eller et tilsynsorgan. Stakeholdere (interessenter) kan være folkevalgte organer, kommersielle aktører, arbeidstakere, underleverandører - det handler om mennesker/grupper som har interesse for saken (Aven, 2015, s. 146 - 147). Som vi ser av modellen under har beslutningstaking en sentral plass i rammeverket:



Figur 1.1: Rammeverk for risikostyring. (Aven, 2015, s.146).

Grunnet oppgavens begrensede omfang beskrives ikke alle elementene i detalj, men ser videre dypere på hva risikostyring og beslutning er.

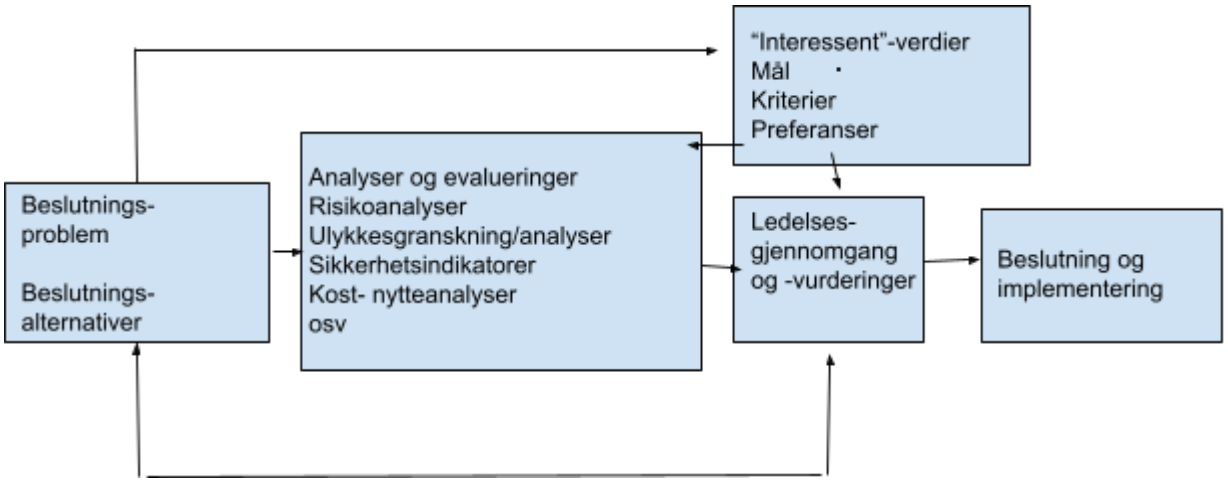
2.1.3 Risikostyring og beslutningstaking: Suksessfaktorer i risikostyringen

Risikostyring foregår rundt oss og overalt i samfunnet hver eneste dag. Om det er lysregulering over et fotgjengerfelt, brannvarslere eller sikringstiltak i en båthavn handler det om forsøk på å styre risiko. Det er ikke alltid det defineres eller omtales som risikostyring, selv om det er dette som skjer. Risikostyringens oppgave er å forhindre, redusere og endre konsekvensene som er identifisert gjennom risikovurderinger (Aven & Renn, 2010). Ved å balansere det å utforske muligheter på den ene siden og å unngå ulykker og katastrofer på

andre siden handler risikostyring om å få innsikt i risikoforhold, vurdere effekt av tiltak og få innsikt i metoder, prosesser og strategier for å kunne kartlegge og styre risiko (Aven, 2015).

Oppgaven undersøker spesifikt hvilke faktorer som bidro til å ikke betalte pengekravet. Aven (2015) diskuterer viktige faktorer for å få til god risikostyring, han skriver *«med risikostyring forstås alle tiltak og aktiviteter som gjøres for å styre risiko»* (Aven, 2015, s. 13). Knyttet til denne studiens drøftingskapittel vil et viktig bidrag være å drøfte hvilke beslutningsfaktorer som var avgjørende for å ikke betale. Ifølge Aven (2015) kan beslutninger vurderes ved å se på resultatet i ettertid. Det kan gi verdifull lærdom for fremtiden, men at en slik metode samtidig er reaktiv da metoden ikke støtter beslutningstaker i beslutningssituasjonen. Å vurdere prosessen på den måten vil gi en større mening (Aven, 2015, s.17).

I Avens modell (2015) starter det med beslutningsproblemet, boksen øverst til venstre er alle interessentene en virksomhet omgir seg med. I midten handler det om hvilke evalueringer og analyser som gjøres, derpå ledelsen/beslutningstaker gjennomgang og endelige beslutning. Beslutningstaker kan enten være styret eller en person i en virksomhet som har myndighet til å beslutte innen deres ansvarsområde. Basert på disse elementene har Aven utarbeidet en modell for beslutningstaking under usikkerhet (Aven, 2015, s.18):



Figur 1.2: Modell for beslutningstaking under usikkerhet. (Aven, 2015, s.18).

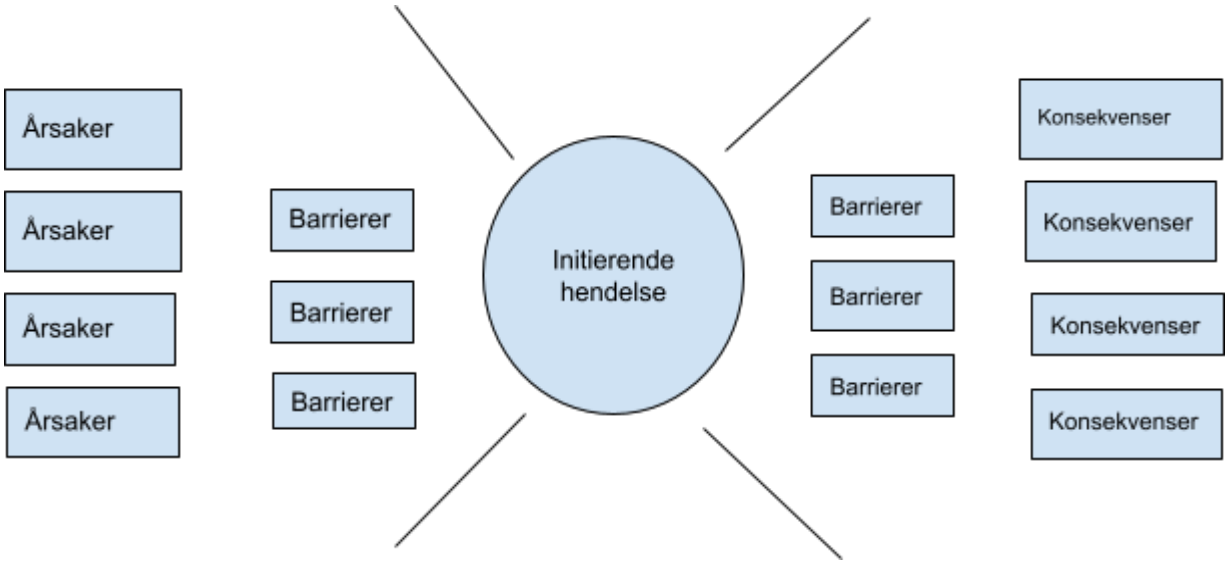
Som vi ser av modellen kan både beslutningstaker og interessentene påvirke beslutningsprosessene (Aven, 2015, s.18). Videre handler det om hvilke vurderinger som gir beslutningsgrunnlag og til slutt å se på hvordan beslutningstaker har gjennomgått og vurdert

før den endelige beslutningen ble fattet. Spørsmålet videre handler om hvordan modellen forbedrer beslutningstaking? Aven (2015) viser til at sentrale *suksessfaktorer i risikostyringen* blant annet handler om beslutningsunderlaget. Aven (2015) angir et rammeverk i form av en risikoanalyse som skal representerer et risikobilde som en løsning på dette (ibid). For å teoretisk se nærmere på dette beskrives det hva en risikoanalyse er.

2.1.4 Risikoanalyse

Ifølge Aven (2015) er det overordnede målet for en risikoanalyse å få oversikt over sentrale givere til risiko og å uttrykke usikkerhet (Aven, 2015). En slik oversikt bidrar til at en kan vurdere ulike alternativer og vise hvilken effekt ulike tiltak har på risiko (Aven, 2015). Risikoanalyser gir ikke beslutningen eller det direkte svaret på hva som er løsningen, men fungerer som beslutningsstøtte når valg skal gjøres (Aven et al., 2008, s. 190). Eksempel på en risikoanalyse er sløyfeanalyse, denne presenteres nå og brukes senere i drøftingen. Grunnen til å velge sløyfeanalyse er at den oversiktlig viser forholdet mellom den uønskede hendelsen, årsaken og konsekvens.

2.1.5 Sløyfeanalyse (Bow-tie)



Figur 1.3: Bow-Tie (sløyfe) presenterer risikobildet. (Aven, Røed & Wiencke, 2008, s. 13).

I en sløyfeanalyse plasseres den utløsende hendelsen i midten, mulige årsaker til venstre og mulige konsekvenser til høyre. Dette gir et utgangspunkt for å få oversikt over situasjonen og konsekvensene fordi figuren viser sammenhengen mellom mulige årsaker, mulige

konsekvenser og tiltak som kan iverksettes for å redusere konsekvensene (Aven et al., 2008, s.13-14). Etter å ha gjennomført en risikoanalyse dannes et risikobilde.

Når en i startfasen skal få oversikt over en hendelse er innhenting av informasjon og å etablere en tidslinje et naturlig startpunkt. Å innhente informasjon og å etablere en tidslinje er også det første steget som gjøres i en granskning. Kjellen og Albrechtsen (2017) har skrevet om åtte steg i en granskningsprosess som til sammen utgjør en ulykkesgranskning: «I en ulykkesundersøkelse er første steg å kartlegge alle relevante fakta. Dette trinnet i etterforskningen vil fokusere på tapene og omfanget av skade, hendelsen og tidligere avvik» (Kjellen og Albrechtsen, 2017, s. 56).

2.1.6 Kost-nytteanalyse

I drøftingsdelen vil kost- nytteanalyse bli omtalt og diskutert, derfor presenteres her et avsnitt av hva en kost-nytteanalyse (KN) er. Helt overordnet kan en si at kost-nytte-begrepet samler gevinsten og kan anvendes for å systematisere fordeler og ulemper ved mulige løsninger opp mot hverandre. Aven (2015) peker på at mange ser på slike analyser som «det riktige redskapet for å prioritere og velge blant løsninger" (Aven, 2015, s. 165), men han understreker at «en slik tenkning holder ikke" (ibid). Aven (2015) argumenterer for at KN-analysene «bygger i realiteten på en risikonøytral tankegang som innebærer at du skal styres av forventningene…og at en slik forventningsbasert strategi ikke kan forsvares" (Aven, 2015, s. 166).

2.1.7 Risikoforståelse og risikoerkjennelse

I en artikkel fra 2015 diskuterer Amundrud og Aven at en tilstrekkelig risikoforståelse må foreligge for å håndtere risiko, her greier forfatterne ut om begrepene risikoforståelse og risikoerkjennelse. Risikoforståelse handler om å ha en dypere kunnskap og innsikt i komplekse systemer og organisasjoner, samt å forstå hvordan teknologi og mennesker samhandler. Dette krever tilgang til relevant data og evne til å analysere og tolke informasjonen. Risikoforståelse handler ikke bare om teoretisk kunnskap, men også om praktisk erfaring og personlige egenskaper som evne til å tenke kritisk og å håndtere komplekse situasjoner (Amundrud & Aven, 2015, s. 43).

Risikoerkjennelse ligger dypere enn risikoforståelse, og at risikoerkjennelse er noe som oppnås etter at kunnskapen om risiko har sunket inn (ibid). Amundrud og Aven (2015) definerer risikoerkjennelse som «innsikten og forståelsen av risikoen man står ovenfor» (ibid). Selve kjernen i risikoerkjennelse dreier seg om å etablere forståelse og erkjenne hvorvidt risikoen er akseptabel eller ikke. Neste delkapittel beskriver ondsinnede handlinger og hva som skiller slike hendelser fra ulykker, systemfeil eller menneskelig svikt.

2.1.8 Safety vs Security

Ulykker kan oppstå på en arbeidsplass, men hendelser kan også komme av at noen planlegger skade. I sum handler det om handlingene er ondsinnet, eller ikke. Modellen illustrerer dette, hvor en ytterst til høyre har plassert sabotasje og terrorisme, her er graden av ondsinnede handlinger størst. Venstresiden er hendelser som følge av uplanlagte brudd eller feil.

Ikke ondsinnet handling				**Ondsinnet handling**
Feil	Brudd	Opportunistiske forbrytelser	Organisert kriminalitet	Politisk kriminalitet

Figur 1.4: Avgrensning mellom ´safety´ og ´security´ (Jore, 2017).

Professor Sissel Haugdal Jore på UiS forsker blant annet på terrorisme, og hun beskriver skillet slik: «Avgrensningen mellom security (sikring) sikkerhet og safety (sikkerhet) bør trekkes i forhold til dikotomien mellom ikke-ondsinnet og ondsinnet hensikt, ikke mellom tilsiktet og utilsiktet» (Jore, 2017, s. 123). I denne oppgaven er det den ondsinnede handlingen som definerer security: «Security (sikring) kan defineres som den oppfattede eller faktiske evnen til å forberede seg på, tilpasse seg, motstå og komme seg fra farer og kriser forårsaket av menneskets bevisste, forsettlige og ondsinnede handlinger som terrorisme, sabotasje, organisert kriminalitet eller hacking» (ibid). Når vi nå har fått på plass hva som ligger bakenfor de ondsinnede handlingene, er målet i neste delkapittel å redegjøre hvordan mennesket kan oppleve og reagere når en utsettes for trusler og frykt.

2.1.9 Trussel og frykt

Løsepengevirus kan oppleves overveldende, dramatisk og kan true virksomhetens eksistens. Konsekvenser er tap av persondata, forretningshemmeligheter og skade på tredjepersoner. For å svare på oppgavens problemstilling presenteres teori om hva trussel er og hvordan frykt kan

påvirke handlinger og beslutninger. Jeg velger teori om dette fordi løsepengevirusofrene utsettes for trusler som er fremsatt med hensikt å spre frykt. Martin (2019) skriver om terror og sabotasje og definerer trussel: «Trussel er et produkt av intensjonene og evnene til trusselaktører – med andre ord deres ønske om å forårsake skade og deres praktiske evne til å gjøre det» (Martin, 2019, s. 18). Bergsjø med flere skriver om trusler innen det digitale domenet; «Trussel kan være hva som helst, enten fysisk eller abstrakt, dersom det har potensialet til å negativt påvirke et objekt eller system» (Bergsjø et al., 2020, s. 147). Å forårsake skade eller negativt påvirke går igjen i begge definisjonene. Å negativt påvirke viser til at en med vilje har et ønske om å opptre truende og spre frykt. Bergsjø med flere (2020) omtaler tre faktorer som inngår i en trusselforståelse; kapabilitet (trusselaktørens ferdigheter til å utøve skade), mulighet (trusselaktørens mulighet til å utnytte sårbarheter) og intensjon (ønsket om å utgjøre skade) (Bergsjø et al., 2020, s. 148 - 149).

Professor Mei-Fang Chen ved Institutt for bedriftsledelse ved Tatung universitetet i Taiwan publiserte i 2016 en studie om hvordan frykt appellerer til menneskelig atferd og hvordan fryktappeller påvirker mennesker, deres handlinger og oppfatninger. Fryktappeller kan i min studie om løsepengevirus handle om trusselbrevene som alle ofrene mottok. Trusselbrevene inneholdt instrukser om hvordan virksomhetene, ved å betale, kunne få data i retur. I tillegg ga trusselbrevene klare føringer om å ikke kontakte hjelp eller bistand fra andre, verken politi eller myndigheter.

Chen (2016) undersøkte hvordan frykt og trusler i klimadebatten påvirker holdning- og atferdsendringer til mennesker som utsettes for sterke virkemidler i form av trusler og dramatiske virkemidler. Hun fant at «Frykt er en kraftig, medfødt emosjonell respons på en oppfattet trussel eller farlig hendelse og en sterk motivator for folk til å endre atferd for å avverge et potensielt negativt utfall» (Chen, 2016, s. 3). Allen C. Johnson og Merrill (2010) undersøkte hvordan fryktappeller innenfor konteksten av datasikkerhet og informasjonssikkerhet påvirker sluttbrukernes handlinger. I artikkelen argumenterer forfatterne at funn fra studien «bør kunne generaliseres til virkningen av fryktappeller i alle desentraliserte miljøer der sluttbrukere utøver en viss grad av autonom kontroll over IT-ressurser» (Johnson & Warkentin, 2010, s. 2). Elementene som skal til i en fryktappell handler om «slutninger om alvorlighetsgraden av en trussel, individets mottakelighet for trusselen, samt uttalelser om effektivitet i form av en anbefalt respons og individets evne til å

utføre den anbefalte responsen» (Johnson & Warkentin, 2010, s. 3). Forskerne fant at å påkalle frykt hos mennesker er en effektiv taktikk for å utløse de handlingene som trusselaktørene ønsker (Johnson & Warkentin, 2010). Overført til denne oppgaven handler det videre om hvordan beslutningstakerne oppfattet løsepengeviruset og trusselen om løsepenger. Bidro trusselbrevene til å forsterke frykten? Jeg vender tilbake til dette i drøftingskapittelet, men gjør videre i teorikapittelet et dypdykk om usikkerhet.

2.1.10 Usikkerhet

Vi kan se for oss ulike situasjoner hvor beslutningstakere skal fatte avgjørelser uten å kjenne alle utfall, avgjørelser må tas til tross for store usikkerhetsfaktorer. Et løsepengevirus medfører stor grad av usikkerhet. Terje Aven (2010) mener risikovurderinger i form av sannsynligheter og forventede verdier er for snevert: «Usikkerhetene reflekteres ikke ordentlig. Usikkerhetsvurderinger som strekker seg utover sannsynligheter og forventede verdier bør inkluderes» (Aven, 2010, s. 199). Aven (2010) mener det i mye større grad må tas høyde for usikkerhetsdimensjonen i risikoanalyser: «Usikkerhet er hovedkomponenten i risiko, ikke sannsynlighet. Implikasjonene ville være en mer ydmyk holdning til å vite sannheten om risiko, og et mer balansert perspektiv» (Aven, 2010, s. 210).

Fra dette ser det nyttig å dukke videre ned i usikkerhet. For hva er usikkerhet? En definisjon fra sikkerhetslitteraturen er «a sense of doubt that blocks or delays actions» (Lipshitz & Strauss, 1997, s. 150). Lipshitz og Strauss (1997) har studert beslutningstaking under usikkerhet (naturalistisk beslutningstaking) ved å analysere 102 rapporter om usikkerhet og beslutningstaking og identifiserte tre former for usikkerhet ved beslutningstaking i kriser:

1. Ufullstendig forståelse (ikke ha en tilfredsstillende situasjonsforståelse)
2. Mangel på informasjon (motstridende, ufullstendig, upålitelig informasjon)
3. Handlingsalternativer i konflikt (vanskelig å skille alternativene fra hverandre)

Videre ble det undersøkt hvordan beslutningstakere håndterer usikkerhet; en fant at fem forskjellige metoder:

1. Redusere usikkerhet ved å samle mer informasjon
2. Resonnere basert på antagelser

3. Vekte fordeler og ulemper
4. Forebygge usikkerhet
5. Undertrykke usikkerhet (handle på grunnlag av intuisjon eller «ta en sjanse»)

De fem taktikkene var ifølge Lipshitz og Strauss (1997) bidrag for å håndtere usikkerhet, sette en i bedre stand til å velge og så langt som mulig tilrettelegge for at usikkerhet ikke skulle være til hinder i en beslutningsprosess. Ved å sette opp de tre formene for usikkerhet mot de fem håndteringsstrategiene i en krysstabell fant en at:

1. Utilfredsstillende situasjonsforståelse var assosiert med reduksjon av usikkerhet, informasjonsmangel var assosiert mot resonnering basert på antagelser.
2. Usikkerhet om handlingsalternativ i konflikt var assosiert mot vekting av fordeler og ulemper.
3. Å være i forkjøpet og undertrykke usikkerhet var likt knyttet til alle de tre formene for usikkerhet.

Det finnes metoder som kan bidra til å redusere usikkerhet, spørsmålet er hva som er den aktuelle situasjonen når usikkerhet skal håndteres, i en løsepengeviruskontekst spiller tid en vesentlig rolle; for hvor lenge vil en virksomhet kunne drive videre om en for eksempel totalt er avskåret for å produsere varer? Aarset understreker at til større usikkerheten er i en krise, jo verre oppleves krisen (Aarset, 2010, s. 36). Det fører oss til den andre bolken i dette teorikapittelet om ulike teorier om krise, kriseledelse og videre krisehåndtering.

2.2 Krise

Problemstillingen etterspør hvilke faktorer som bidro til å løse betalingskravet løsepengevirus medfører. Grunnen til at teori om krise og krisehåndtering velges er for å undersøke om situasjonen virksomhetene sto i da de håndterte angrepet samsvarer det med de teoretiske aspektene for krise. Sagt på en enklere måte: Var det krise? Og hva er krisehåndtering?

2.2.1 Hva er krise?

«Begrepet krise kommer fra det greske ordet krisis og betyr avgjørende vendepunkt og/eller plutselig forandring» (Engen et al., 2016, s. 260). Innen sikkerhetslitteraturen finnes flere krisedefinisjoner. En definisjon som det ofte refereres til da Rosenthal med flere (1989) skrev

om krise. Forfatterne foreslo en definisjon som ytterligere var tilpasset sosiale omstendigheter og at overraskelsesmomentet bare var en av faktorene som kunne lede til høy grad av usikkerhet (Rosenthal et al., 1989, s.10). Definisjonen peker på både trusselen, tidspress, usikkerhet og behovet for beslutningstaking: «En alvorlig trussel mot strukturer, verdier og normer i et sosialt system som under tidspress og usikkerhet gjør det nødvendig å foreta kritiske beslutninger» (Rosenthal et al., 1989, s.10). I 1999 nedsatte Regjeringen Bondevik Sårbarhetsutvalget, utvalgets oppgave var å utrede alvorlige sikkerhetsutfordringer mot det norske samfunnet (Stortinget Innstilling Sårbarhetsutvalget nr. 9 2002-2003). I utvalgets rapport fra 2000 presenteres en definisjon på krise hvor sårbarhet, samfunnets funksjoner sammen med trussel er viktige elementer: «En krise er en hendelse som har et potensial til å true viktige verdier og svekke en virksomhets evne til å utføre sine samfunnsfunksjoner» (NOU, 2000, s. 24). Felles for definisjonene er at det foreligger en trussel og en situasjon som kan føre til skade på verdier som mennesket verdsetter. For denne oppgaven og i drøftingen av problemstillingen er det definisjonen til Rosenthal, T`Hart og Charles (1989) som benyttes. Grunnen til det er at den i tillegg til å peke på trusselen mot et system, også inkluderer behovet for kritisk beslutningstaking. For å oppsummere er krise en risikosituasjon som truer verdier og krever en akutt reaksjon fra de ansvarlige for å ivareta truede verdier. De ansvarlige må organisere eller etablere et forsvar for å komme gjennom krisen. Neste del tar for seg teoretiske perspektiver på kriseledelse. Det er relevant for virksomheter som skal lede virksomheten gjennom et løsepengevirus hvor stress og tidsnød er en del av håndteringen.

2.2.2 Kriseledelse

Når krisen er et faktum, må virksomheten organisere seg for å komme gjennom krisen. Magne Aarset (2010) deler kriseledelse inn i tre prosesser som til sammen består av:

- Risikoledelse
- Problemhåndtering
- Krisehåndtering

Risikoledelse handler om å identifisere hva som kan gå galt for deretter redusere risikoen enten med skadeforebyggende eller skadereduserende tiltak. Problemhåndtering dreier seg om at en tidligst mulig avdekker om en hendelse utvikler seg til en krise for så å iverksette tiltak for å forhindre at krisen enten skjer eller redusere skaden om noe har skjedd. Den siste

prosessen handler om selve krisehåndteringen og kommunikasjon under en krise, både internt og eksternt, samt hvordan en kan være forberedt på krise slik at en tidligst mulig kan komme tilbake til normalsituasjonen.

Flin m. fl. (2008) understreker at selve grunnferdigheten i kriseledelse er beslutningstaking. Ferdigheter og kunnskap om beslutningstaking anses som en kritisk faktor når situasjonen er en risiko- eller krisesituasjon preget av stress og tidsnød. (Flin et al., 2008) Magne Aarset (2010) argumenterer for at deltakere i et kriseteam bør utgjøre en gruppe av personer som takler stress, som er samarbeidsorienterte og gode beslutningstakere samt at de har evne til å lytte og representerer ulike kompetanseområder. Gruppen bør ikke ha for mange deltakere da en for stor gruppe kan medføre beslutningsvegring og ansvarsfraskrivelse» (Aarset 2010, s. 270).

En krise er en risikosituasjon som truer viktige verdier og krever umiddelbare handlinger. De ansvarlige utgjør situasjonens kriseledelse. Neste del tar for seg teoretiske perspektiver på kriseledelse. Å etablere en gruppe som skal lede gjennom en krise omtales gjerne som « å sette krisestab», både i dagligtalen og i kriseplanverk og kriselitteratur fremkommer begrepet stab/krisestab. Det er derfor vesentlig å se på hva som menes med en stab. Det gjøres både fordi flere av informantene som er intervjuet bruker begrepet «stab». I sin enkleste form kan en si at stab er en måte å organisere ledelse på. Bruun og Vatne (1990) skriver om etablering av en stab i en organisasjon, de poengterer at styrken en stab fører med seg er at den åpner for deltakelse for eksperter, men at ekspertene opptrer og deltar som rådgivende funksjoner. (Bruun & Vatne, 1990, s. 106 - 107).

En kriseledelse eller krisestab ivaretar flere oppgaver. I den sammenheng er det relevant å se nærmere på betydningen av å motivere. Eid og Johnsen (2018) uttrykker at «å motivere kan forstås som indre prosesser som påvirker retning og styrke på menneskelig atferd og mål» (Eid & Johnsen, 2018, s. 119 - 120). Forfatterne viser til Maslows behovspyramide for å forstå menneskelig motivasjon. Først kommer de helt basale fysiologiske behovene som mat og drikke, derpå trygghet og orden, den tredje er tilhørighet og aksept og til slutt respekt og likeverd (ibid). Forfatterne argumenterer for at modellen kan relateres til operative tjenester og at ledere, ved å ha innsikt i hva som motiverer, kan føre til prestasjoner. «Prestasjoner kan

ses i sammenheng med motivasjon for suksess og tilsvarende unngå mislykkethet» (Eid & Johnsen, 2018, s. 129). I neste bolk er målet å se på teori om krisehåndteringen.

2.3 Håndtering og beslutning

For denne oppgavens problemstilling er det å skulle ta krisebeslutninger relevant, dermed beskriver denne bolken ulike beslutningsteorier og hva som kan påvirke beslutninger.

2.3.1 Krisehåndtering

For å gi en enkel og overordnet forklaring på hva krisehåndtering er, kan det beskrives som summen av alle tiltak som blir iverksatt når en krise har inntruffet. Det handler om å håndtere krisen og redusere konsekvensene for mennesker, miljø, materielle og økonomiske verdier og «innebærer derfor både håndtering av den akutte og uønskede situasjonen som har oppstått, og om å håndtere en del andre forhold parallelt». (Engen et al., 2016, s. 279 - 280).

Videre beskrives det at håndteringen og styring av en krise kan gjøres enten som en desentralisert styring av krisen (bottom-up) eller som en sentralisert styring (top-down). Hvilken tilnærming som benyttes i kriser er avgjørende ut fra krisens omfang og kompleksitet (Engen et al., 2016, s. 304 - 306). En rekke faktorer spiller inn når en krise skal håndteres. Engen et al. (2016) viser til at krisehåndtering innebærer at beslutninger må tas under usikkerhet (Engen et al., 2016). Også Kruke (2015) understreker usikkerhetsmomentet når han definerer krisehåndtering: «Krisehåndtering kan defineres som kritisk beslutningstaking under høy grad av usikkerhet» (Kruke, 2015, s. 180).

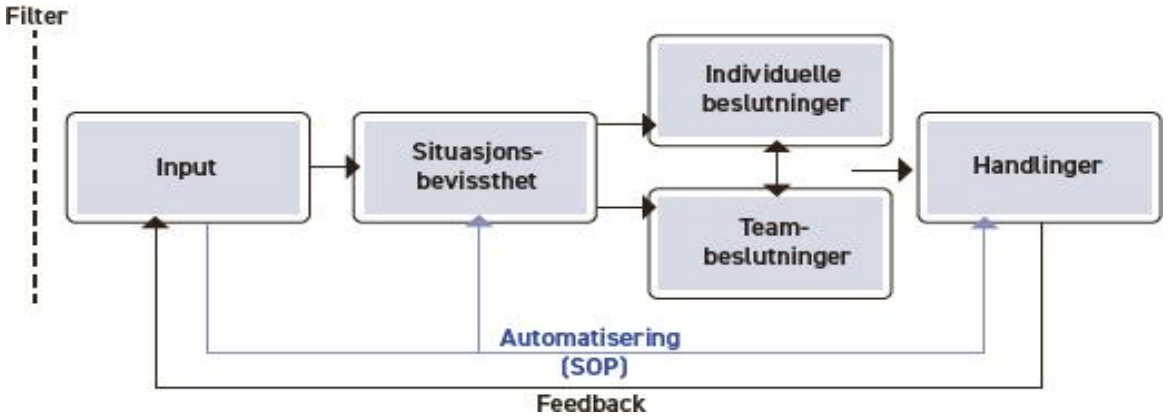
2.3.2 Beslutning i krise

Engen med flere (2016) skriver at når det handler om hurtig utviklende og uventede kriser, der mye står på spill, stiller det beslutningstakere overfor særskilt utfordrende og vanskelige beslutninger (Engen et al., 2016). Videre skilles det mellom intuitive og analytiske beslutninger sett i lys av krisesituasjoner:

Intuitive vurderinger er raske, assosierende, følelsesmessige og ubevisste. Intuitive vurderinger gjøres gjerne tidlig i hendelsen med stort tidspress og lite informasjon. «Når vi resonnerer intuitivt, handler det først og fremst om at vi gjør umiddelbare koblinger og ser

sammenhenger mellom den situasjonen vi nå står overfor, og tidligere erfarte situasjoner» (Engen et al., 2016, s. 313).

Analytiske vurderinger er basert på regler og struktur for resonnement, logikk og bevissthet er mer tidkrevende: «Analytisk resonnering er en mer rasjonell, kronologisk tankeprosess der vi bevisst og logisk avveier ulike hensyn for å komme fram til et best mulig svar eller løsning» (Engen et al., 2016, s. 313). Også Eid og Johnsen (2018) viser til skillet mellom analytiske og intuitive strategier ved beslutningstaking. I den følgende modellen beskriver Eid og Johnsen (2018) hvordan en beslutningsprosess blir til; ledere tar sjelden avgjørelser isolert, men får input fra et team og at de endelige avgjørelsene bygger på «samspill mellom individuelle, mellommenneskelige og situasjonelle forhold» (Eid & Johnsen, 2018, s. 252).



Figur 1.5 **:** Elementene i en beslutningsprosess, individuelt og i team. (Kilde: Eid & Johnsen, 2018, s. 252).

Videre kan beslutningstaking defineres som prosessen for å komme frem til valg eller beslutninger for å møte en gitt situasjon (Flin, O'Connor & Crichton, 2008).

Flin m. fl. (2008) viser til at selve grunnferdigheten i kriseledelse er beslutningstaking og at ferdigheter innen beslutningstaking utgjør en kritisk faktor når det er en risiko- eller krisesituasjon som preges av stress og tidsnød. (Flin et al., 2008). Engen (2016) og Eid og Johnsens (2018) system om analytisk og intuitiv beslutningstaking sammenfaller med Daniel Kahneman (2012) som i sin forskning beskriver system 1 og 2. Jeg tar med Kahneman sin beskrivelse da hans bidrag gir en god og oversiktlig beskrivelse av hvordan menneskehjernen fungerer på to måter. Kahneman skriver om hvordan mennesket vurderer og velger, og videre om hvilke faktorer som spiller inn når beslutninger skal fattes. Kjernen i Kahnemans arbeid

dreier seg om hvilke systematiske feil og svakheter som finnes i menneskets intuitive oppfatning av virkeligheten rundt og hvilken betydning disse kan få for beslutninger som tas.

Kahneman bruker betegnelsene «system 1» og «system 2» for å beskrive de to systemene i hjernen. Kahneman beskriver at begge systemene er utstrakt i bruk i psykologien, men at han i boken utdyper de to systemene og «går lengre enn de fleste» (ibid).

System 1 virker automatisk, intuitivt og hurtig. Her er det liten eller ingen anstrengelse og ingen særlig motstand.

System 2 tildeler oppmerksomhet til de anstrengende mentale aktivitetene som krever det, inkludert komplekse utrekninger. Aktiviteten til system 2 assosieres ofte med en subjektiv opplevelse av valg og konsentrasjon. (Kahneman, 2012, s. 26 - 27).

Kahneman viser til at både system 1 og system 2 er aktive så lenge vi er våkne (Kahneman, 2012, s. 30). System 1 kjører automatisk hele tiden, system 2 er for det meste i hvilemodus. Kahneman beskriver at «System 1 genererer fortløpende forslag til system 2, det handler om intuisjoner, intensjoner og følelser. Hvis system 2 godkjenner dem, blir inntrykk og intuisjoner til overbevisninger og impulser blir til viljeshandlinger» (ibid).

«Når system 1 møter vanskeligheter, påkalles system 2 for å bidra med mer detaljert og spesifikk bearbeiding som kan løse det aktuelle problemet» (ibid). Men dette systemet har imidlertid også en del svakheter, og det er disse Kahneman beskriver hvorfor det er særlig viktig at en har kunnskap om og er oppmerksomme på.

Kahneman beskriver «Priming»-effekten. Det handler om hvordan assosiasjoner bidrar til å skape en «kognitiv letthet» av at noe oppleves som sant, godt eller uanstrengt. Kahneman viser til flere eksempler, han forklarer at system 1 ofte leverer inntrykk som blir til overbevisninger. Faren er at slike assosiasjoner og overføringer bidrar til senket årvåkenhet og at det fører til at system 2 ikke tilkalles for å få en mer kritisk gjennomgang når valg og beslutninger skal fattes. Priming begrenser seg ikke bare til gjenkjennelsen av begreper eller ord, men alt fra bilder, ansiktsuttrykk, hendelser og synsinntrykk. Kahneman forklarer at det som skjer er at system 1 leverer inntrykk som blir til overbevisninger og derav blir system 1 opphav til systematiske feil i intuisjonene» (Kahneman, 2012, s. 67).

En annen effekt som påvirker system 1 er heuristikker, ofte omtalt som kognitive snarveier. Heuristikker bidrar til å skape systematiske skjevheter. Heuristikkene kan kort oppsummeres som tilgjengelighetsheuristikken (en husker bedre hendelser som nylig har skjedd), ankring (det skjer en justering av vurderinger og forslag) og representativitetsheuristikken (slutninger trekkes basert på noe som har vært sant/tilfellet tidligere).

Kahneman viser med dette hvordan system 1 kan påvirkes gjennom priming og heuristikker. System 1 betegnes av Kahneman som naivt og impulsivt, det er system 2 som tviler og gjør mer dyptgående analyser.

Andre feilkilder knyttet til system 1 er evnen til å overdrive. «Overdreven emosjonell koherens», også beskrevet som glorieeffekten. Effekten beskrives av Kahneman som personlige kjennetegn som oppfattes som tiltrekkende og som igjen oppfattes som positive, det kan være intelligens, troverdighet eller empati. Her kan også assosiasjoneffekten spille en rolle ved at, for eksempel ved et førsteinntrykk, kan en få assosiasjoner til hvordan en umiddelbart oppfatter en person (Kahneman, 2012, s. 92).

Kahneman (2012) viser til det han omtaler som «egosvekking». Utover en arbeidsdag kan evnen til bevisst tenkning, konsentrasjon og selvkontroll bli mer krevende, og derav kan «egosvekking» oppstå (2012). For å oppsummere omtaler Kahneman system 1 som et intuitivt og godtroende system som i utgangspunktet ønsker å tro på det som presenteres. Det er system 2 som tviler og forkaster. Er system 2 enten svekket eller opptatt med annet, kan det medføre svakere kontroll. Nøkkelen for å blokkere eller begrense feil fra system 1 er å identifisere tegnene på at en er i et kognitivt minefelt, tenke langsomt og kople på system 2 for å sikre mer robusthet til valg og beslutninger (Kahneman, 2012, s. 447).

2.3.3 Beslutningstakere i møte med eksperter i krisesituasjoner

Krisehåndtering innebærer å ta vanskelige valg preget av trussel, usikkerhet og tidspress. Behovet for å redusere usikkerhet og mestring av krisens kompleksitet krever innspill av av ekspertrådgivere i en beslutningsprosess. (Rosenthal & ’t Hart, 1991). Rosenthal og ’t Hart (1991) har analysert dynamikken mellom beslutningstakere og ekspertrådgivere fra krisestyring, hvilke atferdsmønster som påvirker beslutningstakere og rådgivere i krisehendelser og deres innvirkning på forholdet mellom råd og beslutning.

Et poeng som trekkes frem og diskuteres er forholdet mellom ekspertene og beslutningstakerne. Ekspertene på sin side trenger å bli oppmerksom på den individuelle beslutningstakernes forskjell i ytelse, uformelle og improviserte karakterer av beslutningstaking som på ulike måter kan bidra til å begrense effektiviteten av å formidle sin kompetanse. Tilsvarende bør beslutningstakere i krise ta i betraktning at kriserådgivere heller ikke er immune mot organisatorisk, politisk og psykologisk press som intensiveres i forbindelse med krisesituasjoner. Det presiseres at «ekspertråd» kun vil være et av flere innspill i beslutningsprosessen, da sentrale beslutningstakere i større grad enn tidligere vil kommunisere direkte med underordnede og lavere rangerte eksperter. (Rosenthal & 't Hart, 1991).

Forfatterne (1991) poengterer at beslutningstakere vil forenes om et felles mål under en krise for å avverge trusselen, men at både beslutningstakere og eksperter påvirkes av stress og usikkerhet i krisesituasjoner, noe som kan føre til mer rigid tenkning og økt bruk av stereotypier og fiendebilder. I slike situasjoner kan eksperter med tidlig innsikt få økt makt og ansvar, men også eksperter kan bli påvirket av psykologiske bias og stress. For å takle krisesituasjoner på en best mulig måte bør det etableres et nettverk av relevante eksperter på tvers av fagfelt. Bruk av motekspertise kan være hensiktsmessig for å unngå gruppetenking og ekspertmonopoler. Det er viktig å klargjøre ansvarsområdene til både eksperter og beslutningstakere og fokusere på funksjonell interaksjon for problemløsning.

Rosenthal og ’t Hart (1991) viser til at krisens akutte trussel kan medføre at ekspertene bli nødt til å ta raskere avgjørelser fremfor å gjøre omfattende analyser av de ulike handlingsalternativene, samtidig kan også ekspertene gå ut over sitt eget kunnskapsgrunnlag. Ekspertrådene, som for utenforstående kan fremstå som objektive og rasjonelle, kan være påvirket av at ekspertene i krisesituasjoner står overfor flere av de samme begrensninger som beslutningstakere gjør (ibid). Oppsummert medfører kriser, både for beslutningstakene og eksperter, en stor belastning. Summen av forholdene fordrer en samlet innsats, og det medfører en viktig betydning for hvordan ekspertene og beslutningstakerne utvikler en forståelse for hverandres roller i beslutningsprosessen (ibid). For å forebygge farene ved gruppetenkning og «ekspertmonopoler» anbefales det å implementere «motekspertise» og tydelig avgrense ansvarsområdet til eksperter og beslutningstakerne slik at det ikke er tvil om

deltakerens ulike arbeidsoppgaver (ibid). Overordnet må det stilles krav til et felles fokus på funksjonell interaksjon rettet mot problemløsning til tross for usikkerheten krisen representerer (Rosenthal & 't Hart, 1991).

2.4 Økonomi

Da denne oppgaven undersøker betalingsdilemmaet som følger et løsepengevirus, ses det som nødvendig å ha med et kapittel om økonomi, samfunnsøkonomi og pengepolitikk. Det er viktig for å avklare: Er det lovlig i Norge å betale løsepengevirus? Svaret på dette er nei, men i det spørsmålet ligger det mye som kan undersøkes. Det ble innledningsvis pekt på at løsepengevirusene medfører betydelige kostnader. Kostnadene kan være av økonomisk størrelse i form av tap av produksjon, omdømmetap, persondata på avveie eller at de stjålne dataene kan sette kritisk infrastruktur og hele samfunn ut av funksjon. Om virksomhetene ikke betaler er det likevel kostbart å rent teknisk skulle gjenopprette skade og komme tilbake til normalen. Hvordan skal samfunn unngå kriminalitet? Vil det være riktig å forby betaling av løsepengevirus? Dette kommer jeg tilbake til i drøftingskapittelet. Men først ses det til relevant teori.

2.4.1 «Å binde seg til masten»

I den gresk mytologien finnes historien om hvordan sjøfolk som ble utsatt for Sirenenes sang endte i den sikre død. Sangen til Sirenene var så vakker at skipene som kom i nærheten grunnstøtte og sjøfolkene kom aldri hjem igjen (Garborg, 1918, s. 162 - 163.). Men da den greske helten Odyssevs selv ville høre sangen fikk han sjøfolkene til å putte voks i ørene og binde ham til masten, skipet grunnstøtte ikke og Odyssevs og hans mannskap overlevde (Garborg, 1918, s. 165 - 166).

Uttrykket «å binde seg til masten» har siden blitt en ofte brukt frase om å legge føringer som sterkt bidrar til å begrense valgfrihet eller om mekanismer som hindrer en i å sette kortsiktige hensyn foran langsiktige. Ville det vært klokt av norske myndigheter å «binde seg til masten» og slik sørge for en konsekvent politikk i diskusjonen om å forby betaling av løsepenger?

2.4.2 Den økonomiske politikkens tidskonsistens

I 2004 mottok nordmannen Finn Kydland og amerikaneren Edward Prescott Nobelprisen i økonomi for to artikler de skrev sammen som begge handlet om makroøkonomi som er læren om de store sammenhengene i økonomien. I den ene av de to prisvinnende artiklene, «Rules Rather than Discretion: The Inconsistency of Optimal Plans» (1977) peker Kydland og Prescott på at det vil være fordelaktig for myndighetene å innføre klare, troverdige og forutsigbare regler for politikken. Sentralt står tidsinkonsistensproblemet «When we do have the prerequisite understanding of the business cycle, the implication of our analysis is that policymakers should follow rules rather than have discretion» (Kydland & Prescott, 1977, s. 15). Tidskonsistens innenfor økonomisk politikk handler om at det vil være en fordel for politikere å «binde seg til masten» når en beslutning er fattet og aldri vike fra avgjørelsen.

2.4.3 Å betale - eller ikke betale - hva sier loven?

Ulike land verden over har gjennom tidene diskutert strategier for å håndtere datakriminalitet. Den amerikanske delstaten New York har innført en lov som forbyr statlig virksomhet å betale løsepenger som følge av løsepengevirus, straffen er satt til USD 10 000 for brudd på forbudet (Senate Bill, 2021, S6806). Australske myndigheter har som mål å bli verdensledende innen cybersikkerhet innen utgangen av 2030 (Australian Cyber Security Strategy, 2022). Landet har allerede innført strenge straffer for dataangrep. Rammes landets kritiske infrastruktur er strafferammen satt til 25 års fengsel (Ransomware Action Plan, 2022, s. 14). Et strategidokument er i skrivende stund på høring, dokumentet inkluderer et helt nytt lovforslag om å gjøre det ulovlig for virksomheter som utsettes for løsepengevirus å betale løsepenger (Australian Cyber Security Strategy 2023 - 2030, s. 24). I Norge finnes det ingen unik paragraf i lovdata (Norges lovtekster) som spesifikt gjør det straffbart å betale løsepenger til kriminelle, men å bekjempe kriminalitet i det digitale rom er et prioritert område også for norske myndigheter. I Hurdalsplattformen (Norges nåværende regjering bestående av Arbeiderpartiet og Senterpartiet) omtales bekjempelse av datakriminalitet både som et prioritert område og som et viktig mål for regjeringen (Hurdalsplattformen 2021 - 2025, s. 65).

2.4.4 Løsepengepolitikk

Hvordan myndigheter land over forholder seg til gisselsituasjoner kan selvsagt ikke overføres direkte til dataangrep, i gisselsituasjoner står det om menneskeliv, i dataangrep tas data som

«gisselvare». Det kan likevel være interessant å undersøke hvilke erfaringer som finnes angående løsepengepolitikk. I januar 2017 publiserte Christopher Mellon, Peter Bergen og David Sterman (2017) en studie hvor de undersøkte vestlig gisselpolitikk opp mot myndighetenes løsepengepolitikk (Mellon et al., 2017, s. 3). Studien viste at land som hadde inkonsistente retningslinjer for hvordan de skulle håndtere gisselsituasjoner opplevde at det stimulerte til mer gisseltaking. Forskerne eksemplifiserer funnet ved å gjøre en historisk gjennomgang av Frankrikes forhandlingspolitikk på området: Etter at den franske regjeringen i 2010 fraviket prinsippet om å ikke bistå i gisselsaker, men grep inn for å forsøke å redde den franske hjelpearbeideren Michel Germaneau (franskmann tatt som gissel i Niger av Al-Qaida i 2010) (VG, 2010), opplevde landet en økning i antall gisselaksjoner: Tolv av totalt seksten franske gisseldødsfall skjedde etter redningsforsøket i 2010 (Mellon et al., 2017, s. 5). Frankrike har siden forlatt den inkonsistente forhandlingslinjen med det resultat at antall aksjoner med gisseltaking ble færre (ibid). For å oppsummere viser studien i korte trekk at jo større forhandlingsvilje et land byr på, desto flere angrep risikerer en, samtidig som forhandlingsvilje kan gi en større mulighet til å redde gisler i hvert tilfelle. Ingen forhandlingsvilje, derimot, vil redusere angrepsviljen over tid fordi gisseltakerne skjønner at det ikke er noe å hente, men man risikerer at gisler blir drept i de første angrepene (ibid).

3.0 Metode

I dette kapittelet presenteres oppgavens forskningsdesign og den metodiske fremgangsmåten som er brukt for å svare på oppgavens problemstilling. Valg av forskningsdesign og metode forklares og begrunnes og metodens styrker og svakheter drøftes og vurderes.

Innledningsvis vil jeg først si noe om min rolle som forsker i denne studien. Det er viktig at jeg kritisk diskuterer mitt ståsted til det som undersøkes og vurderer om jeg selv har noen bindinger til temaet. Maxwell (2009) skriver om bias i forskning. Det handler om at innsamling- og analyseprosessen kan bli påvirket av forskerens egne teorier, forståelse eller verdier (Maxwell, 2009, s. 243). Maxwell mener det er viktig å være oppmerksom og bevisst på hvilke forhold som kan påvirke kvaliteten i forskningen, han anbefaler en årvåken, kritisk tilnærming ved at forskeren viser forståelse for egne biaser og hvordan disse kan påvirke forskningen (ibid).

Så hvordan kommer jeg selv ut av dette? Når det kommer til forskeren «meg» og mitt forhold til oppgavens tema oppsummerer jeg min egen rolle slik: Jeg har aldri vært utsatt for dataangrep eller løsepengevirus, ei heller virksomheten hvor jeg jobber eller noen jeg kjenner rundt meg har vært utsatt for løsepengevirus eller blitt frastjålet data eller digitale tilganger. Jeg har dermed ingen personlig erfaring eller egen opplevelse av hvordan det kan oppleves å ikke ha tilgang til sine data. Jeg kan likevel være påvirket av fenomenet, dermed er det nødvendig å være bevisst gjennom oppgaven og i møte med informanter om egne biaser. Jeg har lest flere saker om temaet, i forbindelsen med denne studien har jeg gjort dypdykk i forskning om temaet og lest en rekke artikler og bøker om dataangrep og løsepengevirus. som nevnt innledningsvis var det jo det korte og tilfeldige møtet med «mannen i vinduet» som var anslaget for oppgaven og den valgte problemstillingen. Med dette som bakteppe er det nødvendig at jeg har med meg forståelsen av min egen rolle og utfordrer denne regelmessig gjennom mine møter med informanter, bearbeiding av data, analyse og i skriveprosessen. Videre for metodekapittelet beskrives nå hva et forskningsdesign og hvilke valg som er gjort for å svare på problemstillingen.

3.1 Forskningsdesign

I et forskningsdesign handler det om å designe en overordnet plan som beskriver fremgangsmåten for hvordan problemstillingen skal belyses og besvares. Yin (2018) definerer et forskningsdesign som «en logisk plan for å komme seg herfra til der, der **her** kan defineres som det opprinnelige settet med spørsmål som skal besvares og **der** er konklusjonene» (Yin, 2018, s. 26). Målet er å designe et rammeverk for datainnsamling som legger grunnlaget for en analyse for så å trekke slutninger. I neste delkapittelet redegjøres det for valg av forskningsdesign

3.1.1 Valg av forskningsdesign

Det er for denne oppgaven brukt et en kombinasjon av et eksplorativt (utforskende) og et deskriptivt (beskrivende) forskningsdesign. Utgangspunktet er oppgavens problemstilling som åpent undersøker hvilke faktorer som var avgjørende for å løse håndteringen av betalingskravet løsepengevirusene medfører. Siden det er problemstilling som er førende for hvilken retning en studie tar, vurderes denne oppgaven å treffe kombinasjonen av de to forskningsdesignene. Først hadde jeg en utforskende tilnærming ved at jeg undersøkte hvilken forskning som fantes på området fra før. Det var viktig for å undersøke eksisterende

kunnskapsstatus og sette min forskning inn i en større sammenheng; hva visste vi i Norge om betaling av løsepengevirus?. Silkoset med flere (2021) skriver at selve formålet med et utforskende design handler om mer enn å forstå og tolke dagens situasjon, det handler også om å utvikle hypoteser som kan benyttes i undersøkelser som bygger på et annet design (Silkoset et al., 2021, s. 70). For denne studien var det hensiktsmessig å bygge videre på et deskriptivt design. Hensikten med et deskriptivt design er å beskrive situasjonen på et bestemt område (Silkoset et al., 2021, s. 72). Et eksempel på det, i denne oppgaven, er å se på hvilke vurderinger som er gjort på tvers av flere utvalgte case der alle «casene» løste samme type problem/utfordring. Yin omtaler dette som et multiple case-studie, designet skal inneholde en plan og besvare: «hvilke spørsmål som skal studeres, hvilke data som er relevante, hvilke data som skal samles inn og hvordan disse skal analyseres». (Yin, 2018, s. 26).

Videre velges en induktiv tilnærming fordi en slik tilnærming tar forskningen fra empiri til teori. En induktiv tilnærming betyr at forskeren samler inn data med et åpent sinn (Malterud, 2017), og unngår at teori leder vei for forskningen. Det innebærer at det ikke aktivt er brukt en bestemt teori som utgangspunkt for verken intervjuguide eller analyse. I møte med informanter har spørsmålene vært åpne, og i utvalg av sitater fra informantene og videre med å identifisere suksessfaktorene er det jobbet med utgangspunkt i dataene, det vil si induktivt.

Med utgangspunkt i problemstillingen gjennomføres studien som en komparativ casestudie, hvor case som metode ses på som et verktøy for å undersøke en bestemt hendelse i dybden. Svaret på hvorfor det er valgt å gjennomføre en kvalitativ studie og videre en komparativ casestudie er fordi det er ønskelig å undersøke casene om løsepengevirus i dybden og se helt inn til nyansene i betalingsdilemmaet. Som beskrevet innledningsvis finnes det lite forskning på hvordan norske virksomheter håndterer betalingsdilemmaene et løsepengevirus medfører. Å velge en slik fremgangsmåte anses som fornuftig for å skaffe mest mulig innsikt, forståelse og kunnskap for å svare på oppgavens problemstilling.

Et mål for oppgaven er generalisering, det legges derfor opp til å forsterke oppgavens eksterne validitet. Dette omtales nærmere i kapittelet om oppgavens kvalitet. Men først beskrives studiens forskningsmetode.

3.2 Forskningsmetode

Hva bestemmer valget av metode? «Det opplagte svaret er at *problemstillingen* bestemmer fremgangsmåten» (Johannessen et al., 2021, s. 51), og videre; «For studenter som skal gjennomføre en undersøkelse vil metodevalg være et resultat både av hva som er best egnet til å besvare problemstillingen, og hva det er mulig å gjennomføre innenfor de fastsatte tidsrammene» (Johannessen et al., 2021, s. 53). I forkant av studien ble det utformet prosjektskisse og fremdriftsplan. Tid og tilgjengelige ressurser ble vurdert i forhold til en realistisk tidsbruk for en helhetlig gjennomføring. Målet med studien er å undersøke hvilke faktorer som bidro til en vellykket håndtering av betalingskravet et løsepengevirus medfører. Det overordnede målet var å skaffe til veie data fra flere caser som kunne bringe klarhet i hvordan flere virksomheter løste en kritisk situasjon. Når en skal gjennomføre en forskningsprosess skiller en normalt mellom to metodiske tilnærminger for innsamling av data, kvantitativ og kvalitativ metode (Larsen, 2007, s. 21). Denne studien har en kvalitativ tilnærming hvor data er hentet inn via semistrukturerte intervju, for å styrke reliabiliteten er det også gjennomført en dokumentanalyse (mer om denne senere). I neste delkapittel redegjøres det for valg av forskningsmetode.

3.2.1 Valg av forskningsmetode

«En metode er en fremgangsmåte, et middel til å løse problemer og komme fram til ny kunnskap» (Andersen, 2013, s. 5). Problemstillingen som er valgt fordrer en utforskende og beskrivende tilnærming. Jeg skal utforske og beskrive hva som skjedde da virksomhetene sto i en krevende situasjon og undersøke hvilke faktorer som medvirket til at situasjonen ble løst uten å etterkomme et krav om betaling. Jeg velger dermed å gjennomføre en case-studie, og begrunner det ut fra Johannessen med flere (2021) som beskriver at «Casestudier er et dypdykk i situasjoner, hendelser eller organisasjoner for å undersøke fenomener som ellers kanskje ikke hadde kommet til overflaten» (Johannessen et al, 2021, s. 206). Videre anses en komparativ casestudie som formålstjenlig for å forsterke funnene slik at en kan treffe kravene til generalisering og overførbarhet. Valget faller på å gjennomføre en komparativ (sammenlignende) casestudie, valget begrunnes i det kommende delkapittelet.

3.2.2 Komparativ (sammenlignende) casestudie

Ordet case kommer fra latin og betyr «tilfelle». I en casestudie er det ett eller noen få caser/tilfeller som studeres i dybden, en slik undersøkelsesmetode fordrer en detaljert og

omfattende datainnsamling. Yin (2018) definerer casestudier: «en empirisk undersøkelse som undersøker et samtidsfenomen i dybden og innenfor dens virkelige kontekst» (Yin, 2018, s.15). Yin skriver at det er ikke uvanlig at forskeren ønsker å utvide antall caser etter hvert som forskningen tar form, dimensjonering har også vært et dilemma for denne oppgaven. For når er det egentlig nok antall caser?

Yin (2018) mener at presisjon, i form av validitet og generalitetsnivå, er knyttet til en skrittvis utvidelse av antall case. Andersen (2013) beskriver: «Vanligvis gjennomføres de første studiene med en forholdsvis stor grad av åpenhet hvor mulige dimensjoner og konfigurasjoner testes ut. Men gradvis vil studien strammes inn, og oppmerksomheten snevres inn mot å prøve ut foreløpige generaliseringer. Spørsmålet vil slik melde seg; vil et nytt case bidra til å trekke inn andre dimensjoner, eventuelt stramme inn?» (Andersen, 2013, s. 103). Ser en til denne oppgaven er det relevant å undersøke flere caser for å identifisere suksessfaktorer på tvers av casene. Jeg begrunner det slik: Professor ved Universitetet i Oxford, Bent Flyvbjerg, publiserte i 2004 «Five misunderstandings about case-study research». I fem punkt imøtegår han kritikken ved å ta for seg det han mener er misforståelser når det gjelder casestudien. I artikkelen skriver han om kontekstavhengig kunnskap: «Man kan ofte generalisere ut fra et enkelt tilfelle, og casestudiet kan være sentralt for vitenskapelig utvikling via generalisering som supplement eller alternativ til andre metoder. Men formell generalisering er overvurdert som en kilde til vitenskapelig utvikling, mens «eksemplets kraft» er undervurdert». (Flyvbjerg, 2004, s. 228).

Jeg har vurdert om fem caser er nok. Jeg har vurdert det dithen at i en kvantitativ studie ville fem tilfeller vært for lite, men at det denne gang handler om å undersøke hvert enkelt case i dybden, og at fem caser kan treffe kravene til gyldighet, validitet og overførbarhet (mer om dette senere). Følger vi Flyvbjerg (2004) vurderer han at selv en enkelt casestudie kan bidra til forståelse og økt innsikt, under forutsetning at den utvalgte casen er nøye utvalgt til å belyse det nøyaktige fenomenet som skal studeres. Andersen (2013) diskuterer også hvor mange case som er «nok», og at å gå fra fra ett til to – eller en håndfull – case innebærer flere forskjeller med sikte på å generalisere. «Flere case gir mer å spille på, og åpner intuitivt også for en klarere modellorientering» (Andersen, 2013, s. 95).

Ett case mener jeg i denne studien ville vært for tynt. Årsaken til det er at ved bare å studere ett tilfelle kunne en for enkelt tillagt den ene casen vurderinger ut fra for eksempel virksomhetens størrelse, økonomi eller andre særegne forhold. Jeg støtter meg til Andersen (2013) som skriver at «ved å inkludere flere caser åpner en for klarere kriterier for utvelging og design og derfor klarere forbindelseslinjer mellom empiri og teori…det er derfor, i prinsippet, fordeler å hente ved flere caser knyttet til begrepsdannelse, utforskning av prosesser og testing av årsakssammenhenger» (Andersen, 2013, s. 96). Yin (2015) definerer dette som en multipel casestudie og skriver at det er en studie som inneholder mer enn ett enkelt case. Yin argumenterer for at en multippel casestudie ofte anses som mer robust. Tilsvarende oppsummerer han at single casestudier er sårbare fordi «alle eggene legges i én kurv», og enda viktigere; «de analytiske fordelene ved å ha to (eller flere) tilfeller kan være betydelig» (Yin, 2018, s. 61).

Andersen (2013) skriver at i en komparativ studie fokuseres det på noen hovedvariabler og dens sammenhenger, og i en slik sammenligning foreligger det noe felles, uavhengig av de empiriske funnene. En komparativ studie åpner for større presisjon og får frem ulikheter, nyanseforskjeller og mangfold. Forfatteren skriver også at en slik studie i større grad gir mulighet for generalisering (Andersen, 2013). Videre krever casestudie som metode at forskeren er nysgjerrig og evner å stille åpne og relevante spørsmål. Målet er å etablere en god dialog med informantene, uavhengig om det er individuelle intervju eller gruppeintervju (Yin, 2015). Å gjennomføre et intervju krever at en er oppvakt og tilstede under selve intervjuprosessen. Store mengder data skal i etterkant bearbeides og analyseres, det krever også at en har prosedyrer og legger en klar strategi for en slik gjennomføring. I de videre delkapitlene beskrives innsamlingen av data og hvordan dataene er analysert. Først presenteres casene.

3.2.3 Presentasjon av casene/virksomhetene:

For å belyse problemstillingen empirisk har jeg valgt ut fem etablerte, norske virksomheter. Virksomhetene er valgt ut for at de til sammen representerer en bredde i det norske arbeidslivet. Her følger en oversikt over lokalisering, hva de driver med, hvor mange ansatte, hovedaktivitet og driftsresultat for å vise bredden virksomhetene representerer. Det er også tatt med om virksomheten er offentlig eller privat. Deretter følger en kort presentasjon av hver enkelt case med beskrivelse av hendelsesforløpet koplet til løsepengeviruset. Her gjengis

hendelsestidspunkt, omfang, konsekvenser og kostnad. Dette gjøres for å skape nærhet til datamaterialet som er hentet inn, og for å etablere en forståelse for hvilken betydning et løsepengevirus kan ha for dem som rammes.

Bedrift	Geografisk lokasjon	Ansatte	Driftsresultat	Hovedaktivitet
Østre Toten kommune	Kommuneadministrasjon i Raufoss i Innlandet fylke	1300	9, 2 millioner kroner (2022)	Norsk kommune, offentlig
Amedia	Hovedkontor i Oslo. Avdelinger over hele landet	2100	370 millioner kroner (2022)	Mediekonsern, privat
Hydro	Hovedkontor i Oslo. Etablert i 40 land på alle kontinenter	32.000	39,7 milliarder kroner (2022)	Aluminium og kraftprodusent, privat
Stangeland Maskin	Sola kommune	650	208 000 (2022)	Entreprenør, privat
Inocean	Hovedkontor i Oslo, Aker Brygge. Avdeling i Polen	25	6, 4 millioner kroner (2021)	Ingeniørselskap, privat

Tabell 1.1 Oversikt over virksomhetene Kilde: Årsrapporter og Proff Forvalt.

3.2.3.1 Hydro

Natt til tirsdag 19. mars 2019 lammes Hydros IT-systemer av et dataangrep som påvirket driften i flere av selskapets forretningsområder. Angrepet ble først oppdaget i USA, hvorpå den norske konsernledelsen ble varslet. Angrepet medførte driftsstans og kostet selskapet 550 til 650 millioner kroner og en total ombygging av egen infrastruktur (Norsk Hydro, 2020).

3.2.3.2 Østre Toten kommune

Natt til lørdag 9. januar 2021 ble Østre Toten kommune utsatt for et dataangrep. Undersøkelser i etterkant av angrepet utført av KPMG slo fast at det dreide seg om et løsepengevirus hvor trusselaktøren kom inn enten via sosial manipulasjon (phishing) eller via en usikret fjernløsning uten tofaktorautentisering (KPMG, 2021, s. 9). Ingen av de 1300 ansatte i kommunen kunne bruke datasystemene. Personnummer og helsedata kom på avveie.

3.2.3.3 Inocean

En sen lørdagskveld den 26. juni 2021 opplevde ansatte i det norske ingeniørselskapet Inocean å motta «rare» meldinger via Teams. Dette var fortsatt midt under Covid-19

pandemien og Teams var selskapets kommunikasjonskanal. I meldingen ble det opplyst at firmaet var angrepet og data kryptert. Det krevdes 10 millioner i løsepenger for å låse opp.

3.2.3.4 Amedia

Natt til 28. desember 2021 ble Amedia rammet av løsepengevirus. Konsekvensene for landets nest største mediekonsern rammet produksjon av papiravisene, sensitive persondata var på avveie og flere av virksomhetene var over lang tid uten digital tilgang. Kriminelle hadde kryptert data og satte sentrale datasystemer ut av spill. Angriperne la igjen et «visittkort» med instruksjoner om hvordan man kunne betale løsepenger for å få igjen data.

3.2.3.5 Stangeland Maskin

Natt til 15. desember 2022 ble entreprenørfirmaet Stangeland Maskin utsatt for løsepengevirus. Da ansatte kom på jobb var datasystem låst og adganger sperret. Angriperne bak løsepengeviruset krevde femti millioner kroner i løsepenger for å låse opp (NRK, 2023)..

3.3 Intervju

Det er i studien gjennomført fem semistrukturerte intervju. Johannessen med flere (2021) definerer intervjuformen som et «delvis strukturert intervju som har en overordnet intervjuguide som utgangspunkt, mens spørsmål, temaer og rekkefølge kan variere Intervjueren kan bevege seg frem og tilbake». (Johannessen et al., 2021, s. 108)

3.3.1 Semistrukturerte intervju

Jeg har valgt å benytte meg av semistrukturerte intervju fordi det oppleves som en oversiktlig og nyttig fremgangsmåte som hjelper meg som forsker å lede intervjuprosessen. Metoden forsikrer meg om at alle intervjuobjektene svarer på de samme spørsmålene og det tilfører oppgaven forutsigbarhet når svarene senere skal analyseres. Semistrukturerte intervju tilrettelegger likevel for oppfølgingsspørsmål underveis, dette oppleves som en klar fordel da en ikke er «låst» til en fast mal. At spørsmålene er delt på forhånd har nyttige fordeler, intervjuobjektene har mulighet til å forberede seg og slik kjenne på at de møter forberedt samtidig som en kan gjennomføre intervjuene som en samtale med de fordelene det har med seg; intervjuobjektet kan snakke åpnere og friere.

Kvale og Brinkmann (2018) definerer et semistrukturert intervju som «en planlagt og fleksibel samtale som har som formål å innhente beskrivelser av intervjupersonens livsverden med henblikk på fortolkning av meningen med de fenomener som blir beskrevet» (Kvale og Brinkmann, 2018, s. 357). Informantene som er intervjuet kan alle anses som nøkkelinformanter. Johannessen et al. (2021) beskriver at nøkkelinformantene er «de som gir forskeren innsiktsfull og nyttig informasjon, for eksempel om miljøet i organisasjonen og om viktige hendelser…» (Johannessen et al., 2021, s. 69). Motstykket til å intervjue nøkkelinformanter kan eksempelvis være å intervjue tilfeldige personer. I møte med informanter eller intervjuobjekt med særlig kjennskap til en hendelse er det viktig å være oppmerksom på at informantene besitter dybdekunnskap om temaet. Andersen (2006) påpeker at: «ovenfor ressurssterke nøkkelinformanter kan og bør intervjuer derfor være mer aktive og i større grad ta initiativet» (Andersen, 2006, s. 282). Fra her går jeg over til å se nærmere på intervju som metode, hvordan intervjuene ble gjennomført, hvem som er intervjuet og hvorfor.

3.3.2 Hvem er intervjuet?

Informantene til oppgaven er en sikkerhetssjef, to IT-ansvarlige, en kommunalsjef sammen med IT-sjef og informasjonsdirektør. Fire av intervjuene ble gjennomført via videosamtale på Teams, et intervju var personlig oppmøte. Intervjuene varte opp mot et par timer. Intervjuene startet med et åpent spørsmål der intervjuobjektene ble bedt om å beskrive hvordan det ble oppdaget at virksomheten var utsatt for et dataangrep, dette var et bevisst valg da en slik åpning tok informanten med tilbake til den aktuelle hendelsen og vedkommende fritt fikk fortelle om hvordan situasjonen var den gangen. Deretter var det nødvendig å gå dypere inn i hver sak for å få frem detaljert informasjon deltakerne i beslutningsgruppene, situasjonsforståelse, beslutningsprosessene og hvilke vurderinger som førte til hvilke beslutninger. Intervjuene ble avsluttet med å be deltakerne legge til relevante detaljer, jeg ba dem også åpent selv definere hva som var medvirkende faktorer for å ikke betale.

Jeg opplevde at intervjuene gikk fint å gjennomføre, men var oppmerksom på en rekke forhold: En utfordring med kvalitative intervjuer, ifølge Kvale og Brinkmann (2018), er at det kan oppstå asymmetriske maktforhold i kvalitative forskningsintervjuer. Informantene kan holde tilbake informasjon, snakke utenom temaet, eller det skjer feiltolkninger mellom den som intervjuer og den som blir intervjuet (Kvale & Brinkmann, 2018, s. 52 - 53). For å møte

slike utfordringer sørget jeg for at informantene alle var deltakere i beslutningsgruppen og derav tett på hendelsen, vurderingene og den endelige beslutningen om hvordan betalingen ble håndtert. Informantene anses dermed som nøkkelpersoner. Intervjuobjektene var IT- eller sikkerhetsledere eller hadde annen lederbakgrunn i virksomheten, alle med lang yrkeserfaring. Jeg visste ut fra dokumentanalysen (se eget avsnitt) at informantene var tett på de beslutningene som er utgangspunktet for denne studien, jeg ga informantene god til til å vurdere om de ønsket å delta og sendte intervjuguiden til dem på forhånd slik at de kunne forberede seg, samtidig som jeg presiserte at intervjuguiden kunne utvides med tilleggsspørsmål og oppfølgende spørsmål. I tillegg ble det gjennomført en dokumentanalyse for å styrke oppgavens pålitelighet.

3.4 Analyse av data

Dette delkapittelet beskriver hvordan analysen er gjennomført, både analyse av intervjuene samt dokumentanalyse. Derpå drøftes studiens styrker og svakheter og til slutt gjennomgås forskningsetikk og vurderinger rundt denne.

3.4.1 Analyse av intervjuene

Etter å ha gjennomført fem omfattende intervjuer sitter jeg med flere titalls tettskrevne ark med notater. I tillegg har jeg utdraget fra dokumentanalysen. Nå begynner jobben med å analysere datamaterialet.

«Å analysere betyr å dele noe opp i biter eller elementer» (Kvale & Brinkmann, 2018, s. 219). Ifølge Yin (2015) er noe av det mest utfordrende ved casestudier å analysere nettopp disse dataene. Han viser til flere ulike strategier for analyse, men fastholder at det finnes ingen fasit. For å gjennomføre en analyse med høy kvalitet, anbefaler Yin (2015) å ha en generell analytisk strategi. Videre setter han opp en rekke tester som på ulike stadier i forskningen kan anvendes for å styrke en studie (Yin, 2015, s. 164).

For å analysere tekstmaterialet finnes det innenfor kvalitativ forskning diverse fremgangsmåter. Jeg benytter meg av fremgangsmåten til Tjora (2021) som jeg synes er et logisk oppsett for analyse: Tjora (2021) foreslår å kode datamaterialet, han beskriver at målet for koding er tredelt: (1) å ekstrahere essensen i det empiriske materialet, (2) å redusere materialets volum, og (3) legge til rette for idégenerering på basis av detaljer i empirien

(Tjora, 2021, s. 218). Tjora (2021) fastholder at «ved å rendyrke en *induktiv empirinær koding* er det mulig å redusere påvirkningen av forventninger og teorier som enhver forsker mer eller mindre eksplisitt vil trekke med seg inn i analysen (såkalt «mageføelse»)», og at «kodearbeidet basert på empirisk finlesning bidra til en så induktiv førstefase i analysen som mulig» (ibid). I analysearbeidet som følger fremholder Tjora (2021) at kodene skal ligge tett på deltakerutsagn (i intervjuer) og ivareta det spesifikke i materialet. Man kan gjerne bruke ord eller fraser fra materialet som stikker seg ut. Om det er intervjuer man jobber med, kan dette være «virkningsfulle substantiver, aksjonsorienterte verb, stemningsfulle ordvalg, smarte eller ironiske fraser, lignelser eller metaforer, og lignende» (Tjora, 2021, s. 219).

Tjora (2021) legger ikke skjul på at en slik analysemetode er omfattende arbeid, prosessen beskrives med at en starter med det skriftlige tilgjengelige materialet (intervju, feltnotat etc) og oppretter koder. Kodene kan både være «et ord eller frase, en setning, del av en setning, et utsagn, en dialog, eller kanskje et avsnitt i dokumentet» (Tjora, 2021, s. 219). Slik fortsetter en gjennom hele materialet, etter hvert som det oppstår behov opprettes nye koder. Tjora (2021) understreker at alle kodene er generert induktivt med utgangspunkt i analysedata og at kodenes bidrag er «en kilde til å generere idéer som er tett forankret i empirien, i tråd med et induktivt premiss» (ibid). For å legge grunnlaget for caestudier med høy kvalitet anbefaler Yin (2015) anbefaler at for å fem spesifikke analytiske teknikker:

1. Mønstertilpasning - Passer mønstrene sammen?
2. Forklaringsbygging - Analysere casestudiedataene ved å knytte data til de teoretiske antakelsene
3. Tidsserieanalyse - Kronologisk analyse av data i form av enkle, komplekse eller kronologiske tidsperioder - Formålet er å danne bilder av mønstre
4. Logikkmodeller - Kan en bygge logiske resonnementer ut fra svarene?
5. Krysscaseanalyse - samler funn på tvers av en rekke individuelle studier

Den femte og siste analyseteknikken kommer kun til anvendelse ved multiple casedesign. Dette er relevant for denne studien hvor det handler om å se på sammenfallende funn på tvers av flere case. I en krysscaseanalyse vil funnene samles på tvers av casene, det ses etter likheter, ulikheter og mønster mellom de ulike casene (Yin 2015). Ut fra Yins

analysestrategier må valget av å gjennomføre en krysscaseanalyse også ses i sammenheng med ønsket om å styrke studiens indre validitet, altså troverdigheten.

3.4.2 Dokumentanalyse

Datainnsamlingen er utvidet med en dokumentanalyse. Yin (2015) kaller dette for datatriangulering. «En stor styrke ved innsamling av casestudiedata er muligheten til å bruke mange forskjellige kilder av bevis» (Yin, 2015, s. 98).

Yin (2015) anbefaler at en setter opp en casestudiedatabase som i seg selv er et nyttig bidrag både for å dokumentere og organisere de innsamlede dataene. Videre anbefaler Yin (2015) «at ethvert casestudieprosjekt bør strebe etter å utvikle en formell, presentabel database, slik at andre etterforskere i prinsippet kan gjennomgå bevisene direkte og ikke begrenses til de skriftlige casestudierapportene. På denne måten øker en casestudiedatabase markant påliteligheten til hele casestudien» (Yin, 2015, s. 119).

Jeg gir nå en presentasjon av dokumentanalysen. Dokumentene er enten hentet fra artikler publisert hos NRK eller virksomhetenes årsrapporter. Funnene fra dokumentanalysen bidro både til utforming av intervjuguide samt å verifisere opplysninger fra nøkkelinformanter.

Dokumentanalyse

Virksomhet	Dokumenttype	Publisert	Hvor publisert
Hydro	Årsrapport	10.03.2020	Virksomhetens nettside
Østre Toten kommune	Rapport	28.03 2022	Virksomhetens nettside
Amedia	Årsrapport	05.4 2022	Virksomhetens nettside
Inocean	Artikkel	07.7.2021	NRK
Stangeland Maskin	Artikkel	22.12. 2022	NRK

Tabell 1.2 Tabell over dokumenter til dokumentanalyse

3.5 Oppgavens kvalitet

Jeg går nå over til å drøfte studiens treffsikkerhet i forhold til pålitelighet (reliabilitet), gyldighet (validitet) og generaliserbarhet (Tjora, 2021, s. 259). Det handler samlet om oppgavens kvalitet. Det er viktig å kritisk drøfte hvorvidt resultatene er pålitelige, gyldige og

overførbare. Dalen (2004) påpeker at en grunnforutsetning for kvalitativ forskning er: «at mennesker skaper eller konstruerer sin sosiale virkelighet og gir mening til egne erfaringer. Dette innebærer at det ikke finnes en «sann» virkelighet eller universelle lover» (Dalen, 2004, s. 101). Når en som forsker skal beskrive hva som hendte i en spesiell situasjon kan funnene «påvirkes» av at forskeren selv er påvirket (se kapittelet forskeren meg), enten av forskerens ståsted og/eller tolkningen av informantene svar.

På grunn av dette kan det være vanskelig eller utfordrende å benytte standardiserte metoder ved kvalitativ forskning, argumenterer Mehmetoglu (2004), og at dette er en av grunnene til at kvalitativ forskning er kritisert for å ikke oppfylle kriteriene om validitet, reliabilitet og objektivitet på samme måte som kvantitativ forskning (Mehmetoglu, 2004, s. 143). Forskere innen den kvalitative disiplinen har møtt kritikken ulikt: Lincoln & Guba (1985) mener de positivistiske kriteriene må tilpasses til kvalitativ forskning. Jeg vurderer kvaliteten på denne studien etter Lincoln og Gubas (1985) terminologi og gjør derfor en drøfting studiens gyldighet, pålitelighet (reliabilitet), troverdighet (intern validitet) og overførbarhet (ekstern validitet).

3.5.1 Pålitelighet (Reliabilitet)

Reliabilitet handler om at undersøkelsen som er utført representerer virkeligheten. «Reliabilitet knytter seg til undersøkelsens data; hvilke data som brukes, hvordan de samles inn, og hvordan de bearbeides» (Johannessen et al., 2021, s. 256). En utfordring knyttet til reliabilitet og casestudier er at det kan være vanskelig å gjenskape eller etterprøve siden studien bygger på virksomheter som opererer i dynamiske miljø, grunnlaget for datainnsamling er observasjoner eller intervju som gjør at casestudiene er utsatt for påvirkning fra forskerens innsikt, forståelse og tolkning (ibid). Det er viktig å være oppmerksom på at en vurdering, som gjøres av forskeren selv, kan være påvirket av den som forsker. I de fleste tilfeller kan det i forskningen finnes spor av biaser som kan påvirke eller forstyrre vurderingene (Tjora, 2021, s. 86 - 88). Det kan medføre at reliabiliteten og forskningens pålitelighet vanskelig kan testes. For å synliggjøre utfordringer om reliabilitet kan et grep være at forskeren selv er ærlig og åpen om sin egen rolle til temaet som undersøkes. I delkapittelet «forskeren meg» drøfter jeg mitt eget ståsted med utgangspunkt i oppgavens tema og innhold opp mot oppgavens reliabilitet. Dette gjør jeg for å skape bevissthet om eget ståsted, utfordre min tilnærming og valgene som tas. Denne studien

bygger på data fra et sett med intervjuer, men siden antall informanter er relativt få, kan det bidra til å svekke reliabiliteten. For å styrke påliteligheten er forskermaterialet utvidet med en dokumentanalyse (se eget delkapittel). En dokumentanalyse er valgt med den hensikt å rettferdiggjøre antall informanter og slik forsterkes oppgavens troverdighet. Slik tilføres også studien en en supplert grunnforståelse hvor opplysningene fra nøkkelinformantene enten bekreftes eller avkreftes.

3.5.2 Validitet

Validitet forteller oss hvor relevante dataene er for forskningens problemstilling (Halvorsen, 2008, s. 67). For denne oppgaven er det relevant å gå i dybden og utfordre både den indre og den ytre validiteten. Det gjøres for å være oppmerksom på hvilke «metodiske skjevheter» som kan ha betydning eller på andre måter påvirke funnene. Samtidig er det viktig å vurdere hvordan dataene er relevante for forskningens problemstilling. Intervju med nøkkelinformanter, som alle deltok i beslutningsgruppen, øker validiteten. Jeg supplerer dette med en dokumentanalyse for å forsterke validiteten. Kombinasjonen av intervju og dokumentanalyse bidrar til å underbygge studien og forsterke relevans og pålitelighet.

3.5.3 Indre validitet: Det handler om troverdighet

For å utfordre og teste kvaliteten på dataene er målet i dette delkapittelet å vurdere den indre validiteten. Troverdighet og indre validitet går ut på hvor godt en måler det en faktisk ønsker å måle, om funn og resultater i en studie er sanne. «Troverdighet refererer til sannheten som vist, opplevd, erfart og følt av de som studeres» (Mehmetoglu, 2004 s. 145). Johannessen med flere (2021) sier det slik: «Validitet i kvalitative undersøkelser dreier seg om i hvilken grad forskerens fremgangsmåter og funn på en riktig måte reflekterer formålet med studien og representerer virkeligheten» (Johannessen et al., 2021 s. 256).

For å møte kriteriene ble det satt av god tid til intervjuene og jeg erfarte å få en god dialog med informantene, de var åpne og jeg opplevde at de hadde tillit til meg som forsker. Informantene fikk anledning til å bekrefte resultatet av intervjuene ved at jeg tilbød å returnere notater og informantenes svar. Det var viktig at informantene kjenner seg igjen i svarene og etablere en trygghet for at datamaterialet gjenspeiler informantenes svar og virkelighetsoppfatninger. Når casestudien er beskrivende, slik som denne, er mønstertilpasning relevant. (Yin, 2015, s. 175), så lenge det forutsagte mønsteret av

spesifikke variabler er definert før datainnsamlingen (ibid). Yin (2015) viser til at en slik logikk sammenligner et empirisk basert mønster med et predikert (eller med flere alternative prediksjoner). Er mønstrene sammenfallende, kan resultatene hjelpe en casestudie til å styrke indre validitet: «In qualitative research pattern matching lies at the heart of any attempt to conduct thematic analyses» (Trochim,1989, s. 357). Spørsmålet er om en slik mønstertilpasning gjelder kun for eksperimentelle forsøk og kvantitative studier? Trochim mener at «Qualitative research could usefully utilize pattern matching as a rubric for categorizing data» (Trochim, 1989, s. 365).

3.5.4 Ekstern validitet: Det handler om generalisering

Generalisering er viktig for å vurdere om funnene fra en undersøkelse kan generaliseres til andre sammenhenger. Yin (2015) viser til at ekstern validitet bygger på om man kan generalisere utover selve studien, og at problemstillingen har en nøkkelrolle for om man kan generalisere riktig - og på den måten gi oppgaven ekstern validitet (Yin, 2015). Ifølge Thagaard (2013) dreier ekstern validitet seg om i hvilken grad forståelsen som utvikles innenfor én studie, også kan være gyldig i andre sammenhenger (Thagaard, 2013, s. 205) .

Som nevnt innledningsvis er generalisering viktig, det brukes dermed plass til å drøfte generalisering for denne oppgaven. Historisk har diskusjonen hvorvidt det er mulig å generalisere ut fra casestudier versert innen akademia i årtier. Den danske samfunnsforskeren og professoren Bent Flyvbjerg (2004) mener eksemplets kraft er undervurdert, og har formulert det han mener er fem vanlige misforståelser som angår casestudie som forskningsstrategi. En av misforståelsene er at man ikke kan generalisere på grunnlag av et individuelt tilfelle. Legger en Flyvbjerg (2004) og hans forskning til grunn er det mulig å generalisere ut fra casestudier i kvalitativ forskning. Denne studien tar utgangspunkt i en komparativ case-studie. Vi ser nærmere på hvordan generalisering slår ut, ifølge Tjora (2021), han skisserer to former for generalisering i kvalitativ forskning:

Moderat generalisering: Generalisering i strukturell forstand hvor det er opp til forskeren å beskrive i hvilke situasjoner (tider, steder, kontekster og andre variasjoner) resultatene vil kunne være gyldige.

Konseptuell generalisering: Ved å utvikle konsepter, typologier eller teorier som vil ha relevans for andre tilfeller enn dem som er studert.

Tjora (2021) argumenterer at konseptuell generalisering bidrar til at en *hever blikket* fra empiriske caser ved å stille noen spørsmål, slik som: «Om man ser mer generelt på dette, hva handler det om?» Finnes det noen begreper som fanger opp sentrale trekk ved observasjoner og funn? Finnes det noen dimensjoner som kan brukes til å skissere variasjoner i materialet?» (Tjora, 2021, s. 272).

Andersen (2013) skriver også om generalisering i kvalitativ forskning og i casestudier spesielt, han fremholder at generalisering dreier seg ikke «bare om å trekke essensen ut av et gitt datamateriale, men også å utlede nye observerbare implikasjoner av nye eller etablerte generaliseringer» (Andersen, 2013, s. 133 - 134). Videre forklarer han at «Siktemålet er å finne fram til robuste sammenhenger og å utforske essensen i det som etablerer slike dekontekstualiserte stabile mønstre» (Andersen, 2013, s. 117). Andersen forklarer det med at hvis et bestemt mønster gjenfinnes «er det en god indikator på at man er på sporet av noe som er robust» (ibid). I oppgaven som er beskrevet er utgangspunktet fem virksomheter som alle har opplevd å få sine data kryptert og det er fremsatt et trusselbrev. Utgangspunktet har vært å studere casene med å utvikle en klar forståelse for hva som skjedde og fra der identifisere sentrale trekk gjennom analyse. Jeg har nå sett på og utfordret studiens kvalitet. Det er nå nødvendig å beskrive hvordan dataene er analysert.

3.5.5 Styrker og svakheter ved oppgavens metode

En svakhet med metoden kan være at jeg kun har intervjuet en deltaker i hver av beslutningsgruppene, med unntak av Østre Toten kommune der to personer deltok. En svakhet kan være, som Kvale og Brinkmann (2018) påpeker, at informantene ikke husker det som skjedde. Tidslinjen viser når angrepene skjedde:

Utsatt for løsepengevirus

Virksomhet	Måned	År
Hydro	Mars	2019
Amedia	Desember	2021

Østre Toten kommune	Januar	2021
Inocean	Juni	2021
Stangeland Maskin	Desember	2022

Tabell 1.3: Tidslinje for når angrepene skjedde.

Andre forhold å være oppmerksom på er at informantene av ulike grunner holdt tilbake informasjon, ikke ønsket å svare, eller at det skjer feiltolkninger mellom den som intervjuer og den som blir intervjuet (Kvale & Brinkmann, 2018, s. 52-53). For å møte disse utfordringene er det laget en dokumentanalyse. En dokumentanalyse er en analyse av skriftlige kilder. En slik løsning er valgt for å styrke reliabiliteten til forskningens problemstilling. Gjennom denne oppgaven har jeg vært oppmerksom på den indre validiteten ved at intervjuobjektene er stilt åpne spørsmål, intervjuguiden er utarbeidet slik at den tilrettelegger for at informantene kunne snakke fritt uten avbrytelser så lenge de har holdt seg til tema for oppgaven.

En svakhet kan være om spørsmålene i intervjuguiden er for få eller for overfladiske, men her vil jeg presisere at semistrukturerte intervju legger til rette for oppfølgingsspørsmål underveis, og dette har vært brukt. Samtidig, ved å navigere ut fra en intervjuguide som ikke har høy grad av detaljerte spørsmål, sikret jeg at svarene fra intervjuobjektene kan kodes. Til slutt, i det analytiske arbeidet, har det til sammen dannet et grunnlag for en studie med høy kvalitet, også fordi det er jobbet spesifikt med oppgavens validitet og reliabilitet.

3.5.6 Etiske refleksjoner

I sin enkleste form kan en si at etikk handler om forskjell mellom rett og galt. Her gjøres et skille mellom etikk og moral; Etikk handler om det formelle aspektet rett og galt, mens moral i større grad handler om det hverdagslige (Kvale & Brinkmann, 2018, s. 96).

I overført betydning kan det forstås slik at etikk handler om de formelle sidene ved eksempelvis å utarbeide en masteroppgave, den moralske siden dreier seg om hvordan en som forsker fremstår i møtet med informantene. I denne oppgaven er det lagt til grunn en slik tilnærming i møte med informantene som til sammen utgjør ressursbanken for data i denne oppgaven. Både i den direkte kontakten med informantene og behandlingen av deres svar har en slik bevissthet vært viktig, Informantene har alle gitt en utelukkende god tilbakemelding

for å delta og dele av sine erfaringer og vurderinger. Det tolkes på den måten at intervjuobjektene alle har opplevd at formålet og hensikten med å delta har vært verdifull og innenfor troverdige og etiske rammer. Jeg har i tillegg satt meg inn i de forskningsetiske retningslinjene, utarbeidet av De nasjonale forskningsetiske komiteene i 2014 og etterstrebet disse. Menneskene som har deltatt er behandlet respektfullt ved å forklare informantene hvordan jeg jobber og hva som er formålet med oppgaven. Slik har jeg skapt forståelse for saksområdet, og at erfaringene informantene sitter på, er verdifull. Jeg har forsøkt å utforme et forskningsprosjekt som ordentlig ivaretar integriteten ved å opptre ansvarlig, åpent og ærlig overfor medstudenter, veileder og offentlighet (De nasjonale forskningsetiske komiteene, 2014, utarbeidet av Norges Forskningsråd).

4.0 Empiri

I denne delen presenteres de innhentede dataene fra de kvalitative intervjuene. Empirien er strukturert etter en ni-punkts liste som beskriver hvilke kritiske faktorer virksomhetene har beskrevet som har medvirket til å løse en kritisk situasjon da datasystemene var ute av drift grunnet et løsepengevirus. Eksempler fra informantene er tatt med for å beskrive vurderinger og valg de gjorde. Empirien som presenteres legger grunnlaget for den senere drøftingen.

Identifisere suksessfaktorer

Gjennom analysen som gjøres i dette delkapittelet handler det om å identifisere hvilke valg og beslutninger som ble lagt til grunn da fem ulike virksomheter sto i en kritisk situasjon som omhandlet et løsepengevirus. Ved å se på hvilke vurderinger som var tungtveiende i de endelige beslutningene, er målet å identifisere «fellesnevnere» i beslutningsgrunnlaget for å ikke betale et pengekrav som trusselaktører krevde.

4.1 Ta saken på alvor og etablere krisestab

Alle angrepene som er undersøkt i denne studien skjedde på natten, virksomhetene har dermed beskrevet at det umiddelbart etter at hendelsen ble kjent ble etablert en operativ krisestab som fikk i oppgave å løse saken om løsepengeviruset. Bakgrunnen for en slik umiddelbar respons var sakens alvorlige karakter, løsepengeviruset medførte blant annet produksjonstopp, svarte skjermer og at en var avskåret fra å få tilgang til virksomhetens datasystem. I tillegg beskriver informantene at det forelå trusselbrev med detaljerte

opplysninger om hvordan trusselaktørene/angriperne beskrev hvordan de angrepne virksomhetene skulle opptre for å få tilbake data.

For å håndtere den uforutsette og plutselige hendelsen responderte virksomhetene unisont med å etablere en egen gruppe eller en krisestab som fikk i oppdrag med umiddelbart å gå i gang med å løse den kritiske situasjonen.

Krisestabene som ble etablert har i hovedsak bestått av virksomhetens øverste ledelse, sammen med deltakere fra virksomhetens kommunikasjon og IT-avdeling. Viktige oppgaver for krisestaben var å løse saken, ivareta oppdateringer med konserntillitsvalgte, styre, folkevalgte og øvrige ansatte for å sikre de ansattes interesser. Krisestabens hovedfunksjoner har videre vært å ivareta alle utfordringene dataangrepene førte med seg, deriblant å undersøke hvilken data som var på avveie, finne ut hvordan problemet skulle løses og komme tilbake i normal drift. Da denne studien undersøker ofrenes betalingsbeslutninger og hva som har vært suksesskriteriene for å ikke betale, har virksomhetene beskrevet at det har vært avgjørende at saken ble tatt på største alvor fra første stund og at det ble etablert en krisestab med et klart mandat om å løse saken.

Det er i innad i krisestaben diskusjonene og drøftingene om mulige løsninger er gjort. Videre har krisestaben fungert som virksomhetenes faste organ som har håndtert alle problemstillinger dataangrepet har ført med seg, i den grad øvrig konsernledelse eller virksomhetens styre har blitt informert er det krisestaben som har lagt frem sakene i fellesskap. Den ene informanten forklarer det slik: - *Bare få timer senere var den sentrale beredskapsgruppen samlet, den består formelt av mellom seks og sju helt sentrale personer i selskapet vårt, det var her alle beslutninger ble tatt. Etter hvert som saken vokste i omfang og mer informasjon om angrepet ble kjent ble også flere personer trukket inn fra ulike forretningsområder og støttetjenester.*

Informanten forklarer at det ble tatt to viktige beslutninger alt tidlig på morgenen, få timer etter angrepet var blitt kjent: - *Det var at vi ikke skulle betale og at vi skulle gå til backup - systemene våre. Den andre beslutningen var at vi skulle kommunisere ut, altså at vi skulle sende en børsmelding.*

Innad i krisestaben beskriver informantene at det var «takhøyde for å drøfte hva vi holdt på med» og at «det var viktig for oss å ha en fast gruppe slik at alle satt på samme informasjon og slik kjente saken helt fra innsiden».

4.2 Støtte fra ledelsen

Deltakerne i krisestaben som var satt til å håndtere løsepengevirusene, har alle vært en sammensetning av virksomhetens toppledelse, avdelingsledere samt interne og eksterne bidragsytere i form av IT-konsulenter og/eller eksperter. I den grad ytterligere eiere eller personer fra virksomhetens styre er orientert, beskrives av alle som et viktig bidrag at disse har vært støttende.

En av informantene forklarer: - *Eierne, eller hele ledelsen, har vært innom oss mens vi satt i døgnkontinuerlig arbeid for å løse saken.*

En annen informant beskrev at de ble tilbudt personlig middag fra ledelsen utover kveldene. - *De spurte om vi trengte middag. Om de kunne lage middag til oss, og komme ut til oss på kvelden. Vi har og vært og presentert i styret, og alltid opplevd at vi fikk god støtte. Det er viktig når du skal håndtere en slik uoversiktlig og stor sak.*

En annen informant forklarte at stemningen internt i krisestaben var preget av alvoret, men at det likevel var god stemning. - *Dette skal vi klare, det var slik vi tenkte og motiverte hverandre hele tiden.*

4.3 Beslutning under stor usikkerhet

En av suksessfaktorene som er fremtredende, er at alle beslutningstakerne har tatt valg og avgjørelser under stor usikkerhet. Felles for casene er at nær ingen kjente detaljene om hvor mye data som faktisk var på avveie, omfanget av angrepet var ukjent når en besluttet å ikke betale både i form av hvor mye arbeid saken ville medføre og kostnadene for hva den endelige prislappen ville komme på var usikker. Det samme gjaldt for usikkerhet om hvem som faktisk hadde angrepet dem eller hvor lang tid det ville ta for å komme tilbake til normalen. Ei heller var det kjent for ofrene hva det ville medføre for eventuelle tredjepersoner, personer kompromittert av angrepet som følge av persondata på avveie, om en hadde tilstrekkelige sikkerhetskopier (backup), enten god nok eller tilstrekkelig backup, for å sette datasystemet i stand igjen. Å beslutte under stor usikkerhet kan i så måte ses på

som en suksessfaktor, skulle virksomhetene ha ventet til all kunnskap var kjent kunne de kanskje ventet fortsatt. Felles for virksomhetene var at alle forsøkte å etablere en tidslinje for å undersøke når angriperne kom på innsiden av datasystemene.

4.4 Etablere tidslinje

Felles for alle ofrene var at de forsøkte å etablere en oversikt over når angriperne kom inn i datasystemene og ut fra dette identifisere om tilgjengelig backup kunne benyttes uten at dataene var «infisert». For å forstå bedre hvordan tidslinjen var til hjelp, trekker jeg inn svaret til en av informantene:

Svar: *Ja, den var absolutt til hjelp. Det som er interessant er at vi prøvde å avdekke, altså vi ville gjerne vite hvilken backup vi kunne benytte som var ren, altså identifisere backup som kunne brukes fra før angriperne kom inn og begynte å gjøre ting. Vi måtte gå tilbake i tid og se når det var spor fra angriperne, at de var kommet på innsiden av våre systemer. I vårt tilfelle fant vi den helt konkrete datoen for når de kom inn. Det betydde at om vi tok backup fra før den dagen så kunne vi nyttiggjøre denne, at den backupen var upåvirket.*

Informanten forklarer videre at de jobbet for å etablere en tidslinje for å forsøke å få svar på:

1) Er angriperne fortsatt på innsiden av datasystemet?
2) Hvilke data var kryptert/tapt/på avveie?
4) Gi et så riktig som mulig tidsbilde av saken til politiet (anmeldt samme dag) og til Datatilsynet. (Ifølge GDP-lovgivning skal angrep varsles innen 72 timer).

4.5 Ingen garanti

Alle informantene trekker unisont frem at en viktig del av avgjørelsen om å ikke betale, baserer seg på at om en hadde betalt ville det ikke vært noen garanti likevel om en fikk data igjen. Følgende sitater fra intervjuene beskriver argumentasjonen:

- Selv om vi hadde betalt ville vi ikke hatt noen garanti for at de hjelper deg.

- Det de sier er at de gir deg en nøkkel som dekrypterer, men det er ikke gitt at denne fungerer.

- Trusselen var at de legger dataene de hadde stjålet ut åpent om vi ikke betalte. Men selv om vi hadde betalt, er det ingen garanti.

- De har en slik «wall of shame» hvor de legger ut hvem de har vellykket angrepet, og når. Selv om vi hadde betalt kunne de like gjerne lagt oss ut der, det finnes ingen garantier. Det slår avslutningsvis, i trusselbrevet, at om du ikke tar kontakt med dem vil de prøve seg en gang til. Det er et ganske godt trusselbilde.

- Data fra slike angrep omsettes på det mørke nettet. Data fra angrepet kan like gjerne selges uansett om vi hadde betalt. Den biten der har man ikke kontroll på.

Beslutningen om å ikke betale ble også diskutert i Østre Toten kommune. Informantene forteller dette om vurderingene som ble gjort:

- Det ble diskutert: Hva gjør vi i forhold til løsepengeviruset? Vi hadde en gjennomgang internt, hvor også ordfører var med og eksterne rådgivere og da har det seg slik at rent praktisk, at selv om vi betaler løsepenger, er det ikke sikkert at dataene vi får tilbake er de dataene som faktisk ble stjålet fra oss. Og selv om vi hadde fått tilbake dataene var det ikke sikkert at de var i en stand som gjorde at vi kunne raskt komme opp igjen, så det var jo den tekniske praktiske vurderingen rundt det.

En annen informant trekker frem at ved å betale kunne en like godt risikere at nye løsepengevirus kunne skje:

- Det å betale kunne kanskje løse et av problemene, at vi fikk igjen dataene, men det ville ikke løse at inntrengerne alt var på innsiden av systemene våre og at datasystemet vårt var kompromittert. Det var og en viktig del av den vurderingen at det å betale for å få tilbake krypteringsnøkkelen kanskje ville gjøre at vi fikk tilbake noe data, men neste gang de ville ha mer penger kunne de jo kryptere igjen. Det var jo alt inne i systemet vårt og hadde admin rettigheter. Mens vi visste at disse angriperne var inne i nettverket vårt i datasystemet, så måtte vi bygge et nytt system, flytte alle brukerne over og kastet det gamle systemet vi hadde. Da var vi sikre på at angriperne var ute av vårt system. Så bakgrunnen for at vi valgte å ikke betale var at det ville ikke løse problemet vårt og at det var ingen garanti.

4.6 Ikke støtte kriminelle

Vurderingene om at en ikke ønsket å støtte kriminell virksomhet har vært tungtveiende i de undersøkte casene. For å beskrive i dybden hvordan informantene har vurdert dette er følgende sitat tatt med:

- Det avgjørende momentet var rett og slett om vi skulle være med å finansiere kriminell virksomhet med å betale løsepenger, og da ble konklusjonen at det det skulle vi ikke. Selv om det kanskje kunne gjort at vi hadde fått tilbake dataene, og selv om det kanskje var lovlig, så var det ikke etisk riktig å gjøre det. Da valgte vi rett og slett å ikke gå videre med det spørsmålet.

En annen informant beskriver:

- Det andre var en vurdering om det faktisk er lovlig å betale løsepengevirus, eller slike løsepenger. På det tidspunktet var det i hvert fall uklart om det faktisk var lov eller ikke.

En annen informant beskriver at årsaken til at de ikke opprettet kontakt var: *- Det var at vi skulle ikke gi dem noe som helst påskudd til at dette er business. Vi skal ikke feige ut. Dette skal vi klare.*

- På prinsipielt grunnlag var det uaktuelt å gå i dialog, og å betale løsepenger da det bidrar til å støtte organisert kriminalitet. Amedia ønsker ikke bidra til å gjøre slike alvorlige dataangrep lønnsomme for kriminelle (Amedia, 2022).

4.7 Ingen kontakt med angriper

Samtlige av informantene beskriver at de opprettet aldri kontakt med angriperne bak løsepengeviruset. Informantene har forklart seg eksplisitt om hva som ligger til grunn for at de ikke opprettet kontakt, og setter beslutningene sammen med at de ikke ville ha kontakt med kriminelle. En av informantene forklarer:

- Det var at vi skulle ikke gi dem noe som helst påskudd til at dette er business. Vi skal ikke feige ut. Dette her skal vi klare. Det er jeg glad for nå. Det hadde kostet oss, altså det hadde vært dyrere for oss. Kostnadene var ikke så store for å komme tilbake igjen. Å betale de ti millionene angriperne krevde hadde vært mye dyrere, det visste vi jo ikke da vi tok beslutningen, men det viser den oversikten vi har nå.

- På prinsipielt grunnlag var det uaktuelt å gå i dialog eller å betale løsepenger da det bidrar til å støtte organisert kriminalitet. Amedia ønsker ikke å bidra til å gjøre slike alvorlige dataangrep lønnsomme for kriminelle.

4.8 Eksterne bidragsytere

Ofrene har alle støttet seg til eksterne bidragsytere for å løse sakene, samtlige beskriver at ekstern støtte har vært en viktig årsak til at de kunne løse saken uten å betale. De eksterne bidragsyterne har enten dreid seg om IT-selskap som virksomheten har samarbeidet med tidligere, deltakere fra krisestaben har kontaktet andre virksomheten som har vært utsatt for det samme for å søke råd, samtlige av de undersøkte virksomhetene har vært i kontakt med offisielle myndigheter i form av politi, KRIPOS, Datatilsynet eller NSM (Norsk Sikkerhetsmyndighet).

En av informantene beskriver: - *Vi tok kontakt med andre selskaper som vi visste var blitt rammet av tilsvarende hendelse. I tillegg kontaktet vi Norsk Sikkerhetsmyndighet (NSM), og fikk god støtte derfra. Det er jo de som er faginstans i Norge for dette, og så meldte vi umiddelbart til politiet.*

- Jeg kontaktet IT-direktøren i et selskap som var gjennom dette i fjor, jeg ville høre med dem om de hadde noen råd. Han var veldig åpen og ærlig, og hadde tre-fire råd, blant annet å få tak i en sikkerhetsrådgiver, en skikkelig dyktig en. Der tok jeg han på ordet. De jeg ringte til stilte her på en halvtime, de var til sammen fire personer. I tillegg ble jeg oppfordret til, i den grad vi enten vurderte å betale eller ta kontakt med dem, så måtte vi vente og heller se om vi klarte å ordne opp selv.

Utover dette har rollen til de eksterne IT-ressursene også bidratt med alt ifra å forklare angrepet, drøfte faremomenter, risiko og usikkerhetsmomenter.

- Vi så raskt at løsepengevirusets art og omfang krevde ytterligere ekspertise. De eksterne rådgiverne var jo eksperter på dette. For oss var den viktigste ressursen fra dem at de klarte å spore seg helt tilbake hvor dette startet og laget en tidslinje. Det ble en viktig markør når nye beslutninger skulle tas.

4.9 Menneskene bak: Å motivere

Ingen av informantene som er intervjuet har personlig erfaring med dataangrep eller løsepengevirus av en slik dimensjon som de opplevde i disse casene. Informantene har opplyst at de har behøvd bistand fra eksterne ressurser for å løse en kritisk situasjon. Da ingen av informantene selv hadde erfaring eller særlig kunnskap eller innsikt for å forstå eller å håndtere et løsepengevirus i dybden har flere forklart at et av deres største bidrag ble å tilrettelegge for at menneskene som har jobbet sammen i krisestaben kunne fungere optimalt. En av informantene beskriver det slik:

- *Men suksessfaktoren for dette prosjektet, at det har gått så bra, det er menneskene som har vært involvert.*

- *Vi er fullstendig avhengig av gode relasjoner, både til våre tredjeparter, altså de som leverer varer og tjenester til oss, og til de ressursene vi leide inn i prosessen med å håndtere angrepet.*

Å motivere, følge opp og være til stede mens «alt» var kritisk illustreres også med dette sitatet:

- *Vi var på jobb døgnet rundt. Vi sov her inne på styrerommet blant annet. Men suksessen bak historien er mennesker som jobber med saken. Vi er jo avhengige av engasjere de som var her, vårt mandat er kan vi motivere. Det fikk vi også høre i evalueringen der de har evaluert det arbeidet vi har gjort, det viser igjen i stemningen, det var aldri noe surt eller noen ting, alt handlet om pågangsmot og at det var bare å kjøre på.*

4.2.1 De som betalte

Jeg finner ingen norsk forskning som direkte handler om løsepengevirus og vurderinger om betaling (se kapittel tidligere forskning), jeg synes derfor det er interessant å undersøke om det finnes internasjonal forskning over virksomheter som faktisk har betalt. Via en rekke søk i internasjonale, anerkjente forskningsdatabaser identifiserer jeg artikler om temaet hvor det advares mot å betale, samt en rekke studier som dokumenterer at mange virksomheter betaler. For eksempel betalte University of California i San Francisco 1,14 millioner dollar i bitcoins

etter datatyveri og løsepengevirus i 2020 (Tidy, 2020). I et lignende angrep betalte University of Utah 457 000 dollar for å hindre en omfattende datalekkasje (O'Donnell, 2020).

Da oljeledningen Colonial Pipeline i USA ble angrepet i mai 2021 førte det til drivstoffmangel på USAs østkyst (Eaton & Volz, 2021). Til den amerikanske avisen The Wall Street Journal forklarte selskapets administrerende direktør at en ansatt fant løsepengebrevet fra angripere på en en datamaskin i virksomhetens kontrollrom. Grunnen til at selskapet samme kveld utbetalt nærmere 40 millioner kroner i løsepenger var at kritisk energiinfrastruktur var truet og fordi en var usikre på hvor alvorlig angrepet var for systemene og hvor lang tid det ville ta å bringe rørledningen og systemet tilbake i normal drift (ibid). Da den administrerende direktøren første gang offentlig erkjente at selskapet hadde betalt løsepenger, medgikk han at avgjørelsen var kontroversiell. Han uttalte at det var et alternativ han måtte gjøre gitt den kritiske situasjonen, og viste til at Colonial Pipeline leverer omtrent 45 prosent av all drivstoff til østkysten (Eaton & Volz, 2021).

Forskerne Alena Yurina Connolly og Hervé Borrion ved Zayed University i De forente arabiske emirater har forsket på beslutningsprosesser til ofre for løsepengevirus. De undersøkte 41 løsepengevirus ved bruk av kvalitative data og intervju samlet inn fra organisasjoner og politifolk som jobber med nettkriminalitet i Storbritannia. De testet en hypotese om at «ofrene analyserer situasjonen nøye før de bestemmer seg for om de skal betale løsepenger». Forskerne fikk gjennom studien bekreftet at ofrene ofte utførte en kost-nytte-analyse før de bestemte seg for om de skulle betale løsepenger. En kostnadsoversikt over gjenoppretting, omdømmerisiko og potensielle bøter fra myndigheter ble vurdert. Undersøkelsene til Connolly og Borrion (2022) avdekket også at mangel på kunnskap om fenomenet, ofrenes ansvarsfølelse (at offeret følte seg ansvarlig for angrepet ved at virksomhetens sikkerhetssystemet var i dårlig forfatning), ofrene kjente på press, frykt og usikkerhet bidro til at ofrene betalte. I tillegg spilte betalingsevne en rolle (Connolly & Borrion, 2022, s.14).

De viktigste **hindringene** som forskerne fant for å betale var når angriperne krevde et så høyt løsepengebeløp at ofrene anså det som umulig å håndtere det høye beløpet eller at angriperne ikke var i stand til å gi ofrene den informasjonen de trengte for å gå videre med hvordan selve betalingen skulle gjennomføres. Usikkerheten om lovbryteres forsett og om de var til å stole

på og om de faktisk ville returnere data bidro til å gjøre beslutningsproblemet mer komplekst og sammensatt (Connolly & Borrion, 2022, s. 8). Studien ble publisert i mai 2022 i tidsskriftet Computers & Security som anses som et respektert tidsskrift innen IT-sikkerhetsforskning.

Med dette går jeg nå i gang med å drøfte empirien mot valgt teori. Målet for oppgaven har hele tiden vært å svare på problemstillingen som etterspør hvilke suksessfaktorer som bidro til at virksomhetene løste betalingskravet som følge av løsepengeviruset. Drøftingen i den første delen dreier seg derfor om å kritisk undersøke, analysere og granske funnene (faktorene) i dybden.

5.0 Drøfting

I dette kapittelet drøftes de empiriske funnene som ble gjort i forbindelse med analysen av intervjuene samt dokumentanalysen til sammen. Jeg tar også med forskningen som er gjort fra *de som betalte* som ble utbrodert i empirikapittelet. Jeg inkluderer dette for å tilføre bredde og dybde i drøftingskapittelet og fordi det oppleves som et nyttig og relevant bidrag.

Empirien drøftes i lys av det teoretiske rammeverket som ble presentert i kapittel fire. Formålet med drøftingen er å svare på oppgavens problemstilling: ***Hvilke faktorer bidro til en suksessfull håndtering av betalingskravet et løsepengevirus medfører?***

Drøftingskapittelet i denne oppgaven er delt i tre deler. I den første delen bruker jeg samme struktur som i kapittel fire om empirien hvor jeg systematisk gjennomgår hver og en suksessfaktor. Hensikten er å drøfte funnene enkeltvis mot relevant teori for å systematisk belyse problemstillingen. Den tredje delen drøfter suksessfaktorene opp mot en mer helhetlig tilnærming til risikostyring. Grunnen til at det drøftes helhetlig er for å se mer overordnet på problemstillingen. Den fjerde og siste delen brukes til å kritisk vurdere suksessfaktorenes mulige overføringsverdi til andre virksomheter. Grunnen til at dette gjøres er fordi et viktig element i denne oppgaven har vært overføringsverdi, om andre virksomheter kan nyttiggjøre seg funnene som er identifisert gjennom denne studien.

Men aller først, før drøftingen starter i sin helhet, er det nyttig å se til internasjonal forskning som omhandler studier om ofre for løsepengevirus, men om **de som betalte**. Det anses som et nyttig supplement fordi det er med på å vise ytterpunktene mellom å betale og ikke å betale med utgangspunkt i vitenbasert kunnskap når en nå skal gå i dybden på beslutningene ofrene i denne studien gjorde for å håndtere digital pengeutpressing.

5.1 Suksessfaktorene

I denne bolken drøftes suksessfaktorene hver for seg opp mot teori fra teorikapittelet.

Suksessfaktor 1: Ta saken på alvor og etablere krisestab

Alle virksomhetene beskrev hvor viktig prosessen var med at situasjonen ble tatt på alvor og at det raskt ble etablert krisestab. Å ta saken på alvor og etablere krisestab er tett knyttet til krisehåndtering. Virksomhetene definerer løsepengevirusene som en krise og ser seg nødt til å iverksette ekstraordinære tiltak for å håndtere krisen. Ved å sette krisestab viser virksomhetene at de går inn i krisemodus, de må organisere seg for å komme gjennom krisen.

Flin m. fl. (2008) understreker at selve grunnferdigheten i kriseledelse er beslutningstaking. Ferdigheter og kunnskap om beslutningstaking anses som en kritisk faktor når situasjonen er en risiko- eller krisesituasjon preget av stress og tidsnød. (Flin et al., 2008).

For å beskrive dette opererer virksomhetene med ulike begreper, å sette stab, etablere kriseledelse, `krisestaben samlet seg` eller aksjonsgruppe. Begrepene brukes når informantene beskriver virksomhetens umiddelbare respons på hvordan de håndterte hendelsen. Krisestaben involverte deltakere fra virksomhetens toppledelse, ulike avdelingsledere og IT-ressurser både internt og etter hvert eksterne IT-rådgivere eller IT-eksperter. Å etablere en slik gruppe er med på å understreke at virksomhetene tok situasjonen på alvor, det var deres umiddelbare respons på en situasjon som utgjorde en grunnleggende trussel mot virksomhetens eksistens, slik treffer responsen det alle de fem virksomhetene opplevde - det var krise. Situasjonen var usikker, den kom brått og uventet. Handlingene og den akutte responsen kobles til krisehåndteringen alle virksomhetene iverksatte for å håndtere den akutte situasjonen som oppsto da løsepengeviruset var et faktum. En av informantene beskriver den akutte situasjonen slik:

Inocean

Ja. Det kan vi si. Det var jo det da, vi hadde masse prosjekter, det var jo full brems, full stopp.

En kan likevel spørre seg: Var det krise? I teorikapittelet ble det vist til Rosenthal med flere (1989) som definerte krise til å være «En alvorlig trussel mot strukturer, verdier og normer i et sosialt system som under tidspress og usikkerhet gjør det nødvendig å foreta kritiske beslutninger» (Rosenthal, Charles & t´Hart, 1989, s. 10). Informantene har således forklart at de sto overfor en alvorlig trussel; produksjonen av papiraviser ble begrenset (Amedia), produksjon stoppet opp (Hydro), datasystemet var stengt og en hadde ikke tilgang til kritisk programvare og tegninger (Inocean), personsensitiv data var på avveie (Østre Toten kommune) og angripere hadde kryptert data og låst selskapets databaser (Stangeland Maskin). Av disse konsekvensene er både trusselelementene fremtredende og virksomhetenes verdier under press, situasjonene var preget av usikkerhet og tidspress og gjorde at det var nødvendig å foreta kritiske beslutninger. Alle disse elementene utgjorde i sum en alvorlig situasjon som fikk virksomhetene til å etablere krisestab og ta saken på alvor. Det var viktig for å forsøke å komme seg ut av krisen. I en slik setting har informantene forklart at det var av stor betydning at ledelsen viste støtte, nærhet og forståelse. Det drøftes i neste faktor.

Suksessfaktor 2: Støtte fra ledelsen

Under dette punktet drøftes betydningen av støtte fra ledelsen. For mange kan en slik «faktor» fremstå som åpenbar og naturlig. Men flere av informantene har i intervjuene inngående beskrevet og trukket frem helt konkrete eksempler som beskriver hvordan støtte fra den øverste ledelsen har vært en sentral faktor for å ikke betale. En informant trekker frem at eierne av virksomheten han representerer ikke er «særlig datakyndige folk», men at de til tross for dette viste dem støtte og nærhet. En kan tenke seg at det er vanskelig å skulle vise støtte i en sak hvor en kan kjenne på at en har lite å stille opp med. Da er det interessant å se hvor verdifullt det opplevdes for informanten som forteller at ledelsen, til tross for at de ikke var «særlig datakyndige», satte pris på ledelsens bidrag. At ledelsen responderer med akutt handling og mobiliserer tilgjengelige ressurser alt fra start er med på å sette en høy standard for jobben som skal gjennomføres. En av informantene forteller også om ledelsens bidrag i form av å komme innom med middag på kveldene til et arbeidsteam som jobbet døgnet rundt for å løse en krise.

Som en suksessfaktor trekkes det derfor frem for andre fra dette datamaterialet at mangel på kunnskap og kompetanse om det som kan fremstå som en krevende og truende sak kan støtte og hjelp - også i form av middager - hadde en stor verdi for å bidra med hjelp. I denne settingen er det relevant å trekke inn Maslows behovspyramide. I teorikapittelet så vi at Eid og Johnsen (2018) uttrykker at å motivere kan forstås som indre prosesser som påvirker retning og styrke på menneskelig atferd og mål (Eid og Johnsen, 2018, s. 119 - 120). Forfatterne viser til Maslows behovspyramide når det kommer til å forstå hva som motiverer menneskelig motivasjon. Aller først kommer de helt basale fysiologiske behovene som mat og drikke, derpå trygghet og orden, den tredje er tilhørighet og aksept og til slutt respekt og likeverd (ibid). Forfatterne argumenterer for at modellen også kan relateres til operative tjenester og at ledere, ved å ha innsikt i hva som motiverer og fører til prestasjoner. «Prestasjoner kan ses i sammenheng med motivasjon for suksess og tilsvarende unngå mislykkethet (Eid og Johnsen, 2018, s. 129). I neste bolk ses det på suksessfaktor tre som handler om å ta beslutninger når det råder stor usikkerhet.

Suksessfaktor 3: Beslutning under usikkerhet

Å fatte beslutninger når det råder usikkerhet fremstår som en vanskelig oppgave. Om det handler om store økonomiske dispensasjoner, å navigere en båt gjennom en storm eller om en skal løse en trusselsituasjon med store usikkerhetsmoment. I sum handler det om å ta avgjørelser hvor en ikke kjenner utfallet. Mange vil si at en da løper en risiko. I den sammenhengen er det relevant å hente frem Aven og Renn (2010) sin definisjon om risiko:

«Risiko refererer til usikkerheten om og alvorligheten av hendelser og konsekvenser av en aktivitet med hensyn til det mennesker verdsetter» (Aven & Renn, 2010, s. 3).

Årsaken til at jeg henter frem definisjonen er å se nærmere på to ting; å knytte løsepengevirusene til risiko og videre til usikkerheten som oppsto.

Fra definisjonen handler hendelsene og konsekvensene av noe mennesket verdsetter. Hva mennesket verdsetter i denne sammenhengen kan sies av å være kvantifiserbart (økonomi, tap av penger, omdømme) men i tilfellet av løsepengeviruset handler det også om verdier som er

mer skjønnsbaserte, eksempelvis persondata på avveie eller annen personlig data som spres på det mørke nettet.

En virksomhet vil selvsagt verne om sine verdier og vil oppleve det som krevende om noen tar det som er ditt og som en verdsetter, slike hendelser er med på å understreke alvoret i saken. Virksomhetene som er undersøkt i denne studien sto i slike situasjoner, situasjonene var preget av store usikkerheter, de var fratatt eiendeler som de verdsatte og som virksomhetene ønsket tilbake. I tillegg skulle beslutninger tas i et miljø hvor det var fremsatt trusler med den hensikt å spre frykt. I dilemmaet om de skulle betale løsepenger eller ikke, ser vi at beslutningstakerne var under press. Chen (2016) viser i sin forskning til at frykt er en sterk motivator for mennesker til å endre sin normale atferd for å avverge et potensielt negativt utfall (Chen, 2016). Et eksempel på hvordan en av informantene opplevde situasjonen som omhandlet kombinasjonen frykt, trussel og usikkerhet er når vedkommende refererer til trusselbrevet virksomheten fikk i tilknytning til løsepengeviruset:

Det sto avslutningsvis at om du ikke tok kontakt ville de prøve å angripe en gang til. Det er et ganske godt trusselbilde.

Gjennom beskrivelsen er det tydelig at å skulle ta endelige beslutninger er en krevende øvelse. Fra teorien beskriver Lipshitz og Strauss (1997) usikkerhet som «a sense of doubt that blocks or delays actions» (Lipshitz & Strauss, 1997, s.150). Gjennom deres forskning, omtalt som naturalistisk beslutningstaking, har de identifisert tre forskjellige former for usikkerhet ved beslutningstaking i kriser. Det handler om 1) ufullstendig forståelse, (mangler tilfredsstillende situasjonsforståelse), 2) Mangel på informasjon (Motstridende, ufullstendig, upålitelig informasjon) og 3) at handlingsalternativene kommer i konflikt med hverandre (i dette tilfellet skulle de betale - eller ikke?). (ibid)

Overført til virksomhetenes betalinsgdilemma og hva de skulle gjøre for å løse saken passer alle formene for usikkerhet inn. Den ufullstendige forståelsen kobles til kaoset som oppsto da angrepet først ble gjort kjent og en ikke hadde mulighet til å utføre arbeid som normalt (produksjonsstopp hos Hydro), uten mulighet til å gi ut papiraviser (Amedia), persondata på avveie (Østre Toten kommune), kryptert datasystem (Stangeland Maskin) og arbeidsmateriale

stjålet (Inocean), videre beskriver informantene at de manglet sikker informasjon. De visste ikke hvem angriperne var eller om de var pålitelige/til å stole på og til slutt om mulige handlingsalternativ som kom i konflikt med hverandre; skulle de betale eller la være?

Vi kan se kritisk på dette, for kunne virksomhetene gjennomført ytterligere tiltak for å redusere usikkerheten? Og hvordan jobbet de for å redusere usikkerheten? For å komme nærmere et svar er en nyttig øvelse være å ta frem Lipshitz og Strauss (1997) som presenterer fem prinsipielle strategier for å redusere usikkerhet; 1) Samle mer informasjon, 2) Resonnere basert på antagelser, 3) Vekte fordeler og ulemper 4) Forebygge og 5) Undertrykke usikkerhet i form av å handle på grunnlag av intuisjon eller å «ta en sjanse».

De fem håndteringsstrategiene skal ifølge Lipshitz & Strauss (1997) bidra til å håndtere usikkerhet, sette en i bedre stand til å ta valg og så langt som mulig tilrettelegge for at usikkerhet ikke skal være til hinder i beslutningsprosessen. Ved å sette opp de tre formene for usikkerhet mot de fem håndteringsstrategiene i en krysstabell fant en at:

Utilfredsstillende situasjonsforståelse = assosiert med reduksjon av usikkerhet
Informasjonsmangel = assosiert mot resonnering basert på antagelser
Handlingsalternativ i konflikt = assosiert mot vekting av fordeler og ulemper.
Å være i forkjøpet og undertrykke usikkerhet var likt knyttet til de tre formene for usikkerhet.

Vi ser av funnene fra den komparative analysen at alle beslutningstakerne gjør flere øvelser for å innhente mer informasjon; de forsøker å etablere en tidslinje for å få finne ut når angriperne kom inn i datasystemene, det hentes inn eksterne bidragsytere i form av ekspertise og kontakter andre virksomheter som har erfart løsepengevirus. Tiltakene samsvarer med funnene til Lipshitz og Strauss (1997) sin strategi for å redusere usikkerhet. Det handler om å få mer oversikt og mer informasjon om situasjonen på grunn av utilstrekkelig situasjonsbevissthet eller utilstrekkelig forståelse hvor målet er å oppnå en felles situasjonsforståelse. Aarset (2010) understreker at jo større usikkerheten er i en krise, jo verre oppleves krisen (Aarset, 2010, s. 36). Også Aven (2015) understreker betydningen av usikkerhetsintervaller i risikostyringsprosessen (Aven, 2015, s. 63). Aven (2015) skriver at for å kunne styre risikoen på en god måte er usikkerhetsintervaller viktige hjelpemidler. (ibid).

Når en gjennomfører en risikoanalyse, skriver Aven (2015), så gjør en i realiteten en analyse av risiko og uttrykker usikkerhet (Aven, 2015, s. 48).

Tradisjonelt har risiko blitt målt gjennom utregninger ved å kvantifisere sannsynlighet og konsekvens, men fra Aven og Renn sin definisjon *«Risiko refererer til usikkerheten om og alvorligheten av hendelser og konsekvenser av en aktivitet med hensyn til det mennesker verdsetter»* (Aven & Renn, 2010, s. 3) ses et nyere syn som også innehar en skjønnsmessig faktor - hva mennesket verdsetter. Menneskene i denne studien ble utsatt for en aktivitet og fratatt eiendeler som var viktige, med andre ord var usikkerheten sterkt til stede. Gjennom denne bolken er det drøftet gjennom flere teorier og perspektiver hvordan virksomhetene jobbet for å redusere usikkerheten. I det neste kapittelet drøftes dette nærmere, blant annet ved bruk av en sløyfeanalyse (bow-tie-modell).

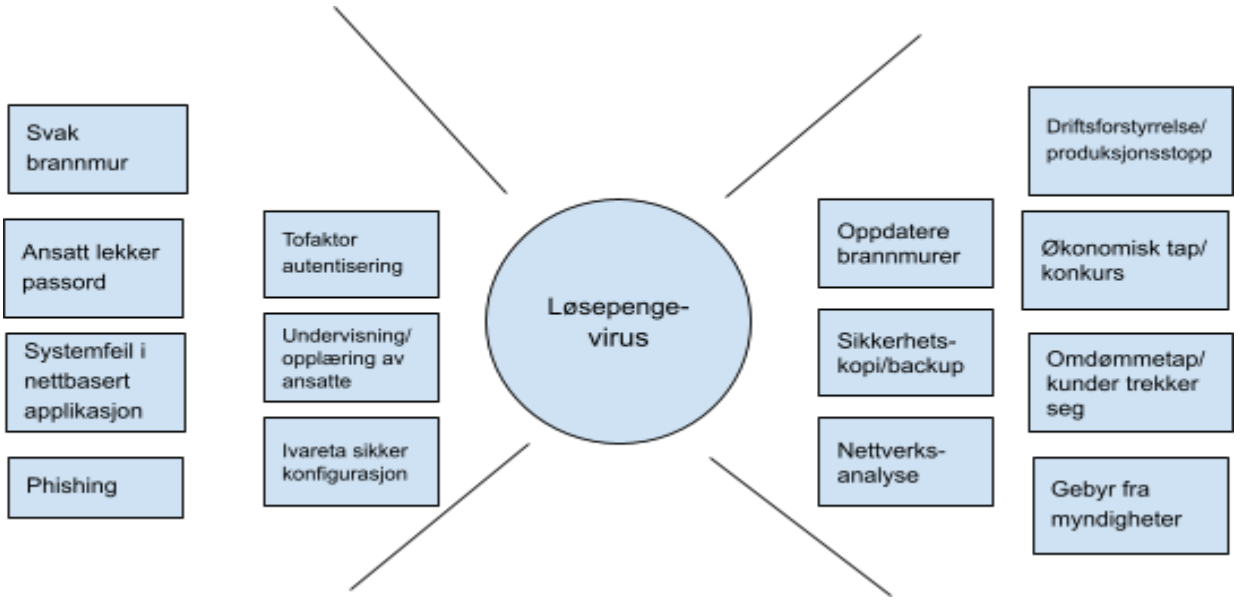
Suksessfaktor 4: Etablere tidslinje for når angriperne kom inn i systemet

Flere av informantene har beskrevet at en viktig årsak til at de ikke betalte var at de tidlig fikk oversikt over når angriperne kom seg inn i datasystemene. Ved å etablere en tidslinje medførte det at virksomhetene kunne ta sikkerhetskopier fra før angriperne var inne i systemet, det gjelder spesielt for dem som kunne identifisere at angriperne ikke hadde vært lenge inne i systemet, som eksempelvis Amedia som fant at angriperne ikke hadde vært lengre «inne» enn et par uker.

Den ene informanten forklarte det slik: *«Om vi tok backup fra dagen før angriperne kom seg inn så visste vi at den backupen var upåvirket, at dataene var gyldige».* En slik vurdering koples direkte til risikovurderingen som ble gjort, for om det hadde vist seg at tidslinjen gikk langt tilbake, at det ikke «bare» gjaldt en uke, men eksempelvis et helt år, ville kanskje risikovurderingen vært en annen. Da ville en kanskje vurdert konsekvensene som tap av data og jobben med å gjenopprette data av en annen størrelsesorden. Den påfølgende konsekvensanalysen ville gjennom et slikt risikobilde sett annerledes ut og beslutningen for hvilken endelig løsning som skulle velges ville muligens vært en annen. En tidslinje fremstår dermed som en viktig faktor som en kunne bidra til å gi mer sikker kunnskap når beslutninger om angrepet skulle tas.

I studien om de som betalte ble det konkludert med at i «hovedsak, før de bestemte handlinger for å betale eller ikke utførte ofre organisasjoner en grundig kost-nytteanalyse ved å bruke all tilgjengelig informasjon om angrepet og de potensielle konsekvensene». Men er bruken av kost-nytte-analyse det mest rasjonelle? Aven (2015) skriver at en må se utover kost-nytte-analyser da slike forventningsbaserte strategier ikke kan forsvares da vi alltid står «overfor usikkerhet om hva som vil være konsekvensene av ulike alternativer» (Aven, 2015, s. 166). Det er dermed relevant å undersøke hva virksomhetene i denne studien gjorde for å komme gjennom krisen.

Å etablere en tidslinje kan ses på som et forsøk virksomhetene gjorde for å finne mer ut av konsekvensene av angrepet. Fra teorien ble sløyfeanalysen (2015) presentert, men i den følgende modellen er den satt opp med funnene fra analysen:



Figur 1.9 Bow-Tie/Sløyfeanalyse for løsepengevirus.

Sløyfeanalysen beskriver risikobildet. Først i form av årsaker som kan ha ført til den uønskede hendelsen (helt til høyre), deretter forebyggende barrierer som kan bidra til at den uønskede hendelsen oppstår (nest til høyre). På venstre side representerer de første boksene konsekvensreduserende barrierer og helt til høyre konsekvensene.

Å etablere en tidslinje er også det første steget som gjøres i en granskning, ved å gjøre en systematisk gjennomgang av hendelsen for å få en så detaljert og fullstendig oversikt som

mulig over hva som har skjedd, settes informasjonen inn i en tidslinje. Kjellen og Albrechtsen (2017) har skrevet om åtte steg som til sammen utgjør en fullskala granskning. De beskriver at «I en ulykkesundersøkelse er første steg å kartlegge alle relevante fakta. Dette trinnet i etterforskningen vil fokusere på tapene og omfanget av skade og skade, hendelsen og tidligere avvik (Kjellen og Albrechtsen, 2017, s. 56). Overført til hva ofrene for løsepengevirusene gjorde fremstår forsøket på å skaffe seg en oversikt over hendelsen og få innsikt i hva som har rammet dem som sentral. Oppsummert kan en si at det alle gjorde var å gjøre en kombinasjon av det som er første steg i en granskningsprosess kombinert med en risikovurdering for å få mer innsikt om situasjonen de sto i for å vurdere risikoen.

Men selv om alle virksomhetene forsøkte å etablere en tidslinje, var det ikke alle som klarte det. Grunnen til at noen av virksomhetene ikke klarte å etablere en tidslinje var fordi systemene var så utilgjengelige at det ikke var mulig å jobbe i datasystemene eller at løsepengeviruset var av en komplisert utgave. Men felles for alle var at de alle forsøkte å etablere en tidslinje. Virksomhetene som klarte å etablere tidslinje rapporterer at det var til hjelp i forhold til dilemmaet om betaling, de kommuniserer selv at det var en viktig suksessfaktor. De virksomhetene som ikke fikk etablert tidslinje gjorde likevel et forsøk fordi de så at kunnskap om angrepet, satt inn i en slik tidslinje, hadde vært nyttig og verdifull.

En av informantene forklarer hvorfor en slik tidslinje var verdifull på denne måten:

«*I vårt tilfelle fant vi den helt konkrete datoen for når de kom inn. Det betydde at om vi tok backup fra før den dagen så kunne vi nyttiggjøre denne, at den backupen var upåvirket».*

Et annet funn er suksessfaktoren som omtales i neste delkapittel «ingen garanti», i sum er det denne faktoren som gis mest oppmerksomhet av samtlige av informantene når de argumenterer for beslutningene som ble gjort i forhold til betalingsdilemmaet.

Suksessfaktor 5: Ingen garanti

Det finnes ulike metoder for å beskrive risiko. En retning er å benytte målinger gjennom matematiske og statistiske modeller (Aven, 2015, s. 63 - 73). Gjennom en slik tilnærming kvantifiseres eller tallfestes sannsynligheten for fremtiden og risiko blir et produkt av sannsynlighet og konsekvens. En annen retning, som kan ses på en nyere, eller mer moderne

metode, er når risiko er mer enn tall og inkluderer skjønnsmessige vurderinger - det handler om hvordan risiko enten forstås eller oppleves. En må da synliggjøre hvilken kunnskap dette bygger på, og hvor sterk kunnskapen er. (Aven, 2015, s. 61).

Hvilken risiko sto ofrene i denne studien overfor da de skulle ta sine endelige beslutninger om å ikke betale? Fra den komparative analysen som ble gjort forut for drøftingen så jeg etter sammenfallende faktorer som til sammen dannet grunnlag for at ofrene for løsepengevirus ikke betalte et løsepengekrav. En av de mest omtalte suksessfaktorene er at selv om en hadde betalt, vil en likevel ikke hatt noen garanti for å få data tilbake. En ville heller ikke hatt noen gyldig eller valid garanti om de eventuelt returnerte dataene var i slik stand at de kunne implementeres tilbake i systemet. Sagt med andre ord; ville betaling av løsepenger vært «value for money»?

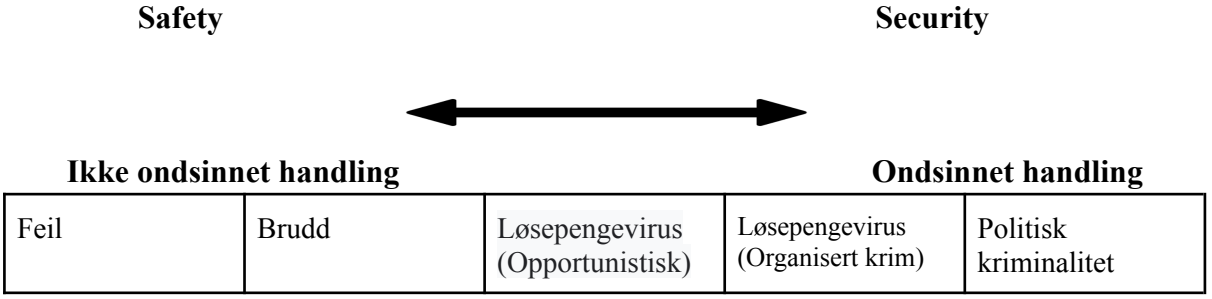
Ofrene i denne studien har alle beskrevet at de mottok trusselbrev fra angriperne og at det ville medføre konsekvenser om de ikke rettet seg etter løsepengekravet. Truslene handlet også om at virksomhetene ville havne på en «shaminglist», en liste hvor selskaper som vellykket angripes «henges ut» og som beskriver «shaming» (skam) ut fra at de var sårbare og ikke hadde et tilstrekkelig forsvarssystem. En av informantene forklarte at de håndterte trusselen slik:

«*Vi kunne betalt, men det var ingen garanti for vi kunne jo uansett havnet på listen likevel*».

Virksomhetene har da alle tatt en vurdering om risikoen de var utsatt for, de har drøftet risikoen og forståelsen av denne i dybden og erkjent hvilke konsekvenser det kunne medføre å ikke betale. Ifølge Amundrud og Aven (2015) er risikoforståelse kunnskapen man har om risikoene, knyttet til en aktivitet, og at risikoforståelse er en forutsetning for å kunne erkjenne og redusere risiko. Videre skiller Amundrud og Aven mellom begrepene risikoforståelse og risikoerkjennelse og argumenterer at for å ta en beslutning om risiko trengs først risikoforståelse og deretter risikoerkjennelse. 'Risikoerkjennelsen' tar risikoen til seg og aksepterer situasjonen (i) og trekker de nødvendige konklusjonene (ii) (Amundrud & Aven 2015 s. 44).

En finner videre konseptet risikoforståelse nyttig i denne settingen. Som Amundrud og Aven (2015) beskriver handler det om «å fange opp det faktum at man «ser de relevante aspektene ved risiko: hendelsene, konsekvensene, usikkerhetene og bakgrunnskunnskapen som ligger til grunn for vurderingene» (Amundrud & Aven 2015 s. 47). For å se dypere inn i denne argumenterer Amundrud og Aven at 'Risikoerkjennelse' handler om «å akseptere risikoen, og gjøre nødvendige konklusjoner og handlinger» (Amundrud & Aven 2015 s. 44). I saken om å betale eller ikke betale et løsepengekrav kan en ut fra en slik teori se samsvar mellom den situasjonen virksomheten sto i og beskrivelsen av nyansene mellom risikoforståelse og risikoerkjennelse Amundrud og Aven (2015) teoretisk beskriver. Det er faktisk en risiko for at lovbrytere ikke vil tilby en dekrypteringsnøkkel, de kunne også kommet tilbake for å be om mer penger senere, eller uansett plassert ofre på en «shaming list», og dermed ville ofrene vært like langt - også om de hadde betalt.

«Ingen garanti» signaliserer også størrelsen på usikkerhetsfaktoren som virksomhetene sto overfor. Som vi så fra teorikapittelet er en vanlig måte å vise hvordan security er forskjellig fra safety er hvordan graden av menneskelige handlinger kan defineres ut ifra om handlingen er ondsinnet eller ikke (Jore, 2017). Den vedlagte modellen fra teorien gjøres også om til en egen for denne oppgaven: Løsepengevirusene plasseres nest til høyre i modellen (opportunistisk - oppnå egen vinning) og over til organisert kriminalitet. Grunnen til det er at løsepengevirusene er ondsinnede handlinger satt i system med formål å true til seg penger, de kan også brukes for å spre skade på kritisk infrastruktur med det formål å ramme samfunn.



Figur 1.10: Avgrensning mellom ´safety´ og ´security´ for løsepengevirus.

Videre kan en se på dette i et usikkerhetsperspektiv på den måten at det er vanskelig å forutsi nøyaktig hva angriperne vil foreta seg da dette handler om menneskelige aktiviteter. Angrepene de har planlagt og gjennomført finnes ikke som åpne planer eller er tilgjengelige via åpne dokumenter som kan leses, lastes ned, studeres og undersøkes. Ofrene var derfor

avskåret fra å få innsikt i handlingene til angriperne, hvordan de tenkte eller hva de planla. I starten av denne oppgaven ble det referert til at Nasjonalt cybersikkerhetssenter (NCSC) har observert en vesentlig økning i hendelser knyttet til krypteringsvirus og økonomisk motivert kriminalitet på nett (Nasjonalt Cybersikkerhetssenter, 2021, s. 8). I det neste delkapittelet er målet å drøfte hvordan ofrene for den type økonomisk kriminalitet vurderte og besluttet..

Suksessfaktor 6: Ikke støtte økonomisk kriminalitet

Flere av informantene oppga at tungtveiende grunner for å ikke betale var ønsket om å ikke støtte kriminell virksomhet. Fra teoridelen om økonomi ble det trukket frem at det ikke finnes forbud eller lov i Norge som direkte forbyr betaling av løsepenger for å løse et løsepengevirus. At virksomhetene ikke ville støtte kriminell virksomhet kan handle om samfunnsansvar, at en ikke ønsker å bidra til å støtte kriminelle aktører som kan anvende pengene til å begå ytterligere kriminalitet eller terrorhandlinger. Ofrene i Østre Toten-angrepet vurderte at å betale ville være uetisk, ofrene i ingeniørselskapet Inocean ønsket å ikke betale - for som informanten sa:

- *Vi skulle ikke gi dem noe som helst påskudd til at dette er business.*

Ville Norge som nasjon opplevd færre løsepengevirus om Norge var et land som **konsekvent ikke** betalte løsepenger? Hvordan ville et slikt prinsipp «virke»? Og ville det i det hele tatt vært mulig å oppnå? Uten direkte sammenligning er det interessant å se til Frankrike som førte en tidsinkonsistent forhandlingspolitikk i gisselsaker, noe som førte til mer terrorisme og gisseltaking. Frankrike har siden forlatt forhandlingslinjen med det resultat at antall aksjoner med gisseltaking har gått ned. Forskerne Kydland og Prescott ble begge tildelt nobelpris i økonomi i 2004 (Kunglige Vetenskapsakademien, Ekonomipriset 2004) for oppdagelsene de gjorde om at klare og faste regler ville medføre en langt mer konsistent politikk enn om politikere og beslutningstakere skulle utøve skjønn for hver sak (Prescott & Kydland, 1977).

I spørsmålet om politikerne bør binde seg til masten og forby løsepengevirus er et annet spørsmål om hvordan et slikt lovforslag skal etterforskes? Skal en aktivt gå etter dem som betaler, eller skal ressursene brukes til å etterforske dem som sto bak angrepene og forårsaket skade? Spørsmålet er jo hva som er positivt med å gjøre det ulovlig å betale? Vil en mestre å kneble datakriminelle og deres aktiviteter? Samfunn verden over har

alltid etterstrebet å komme kriminalitet til livs, hvordan en skal oppnå å strupe virksomhet som har til hensikt å skade og ødelegge innen den digitale verden, vil nok være utgangspunkt for store debatter i fremtiden. Enn så lenge kan det være en fordel å ha mest mulig åpenhet om løsepengevirusene, hvordan de rammer og hvilke konsekvenser det medfører. Åpenhet bidrar til større innsikt i problemstillinger, mer kunnskap kan føre til bedre beslutninger og viktig lærdom av hverandres erfaringer. Om en binder seg til masten og gjør det straffbart å betale vil en kanskje gå glipp av verdifull innsikt som følge av tapt åpenhet og mulighet for innsyn.

Et annet moment som er relevant å diskutere er risiko på virksomhetsnivå. Om ofrene betalte kunne de kommet i en situasjon som kunne medført store økonomiske tap, både i form av å miste kunder som ikke ville samarbeide videre og derav tapte inntekter. Betaling kunne også medført et omdømmetap som kunne satt hele virksomheten i en krevende og alvorlig situasjon da det å betale kan ses på som en direkte oppmuntring til ytterligere angrep og slik kan en bli assosiert med å støtte kriminelle. I sum kunne disse momentene ført til negativ eksponering og forsterket omdømmetap, konsekvensene av dette kunne truet virksomheten på et helhetlig nivå. Det strekker seg lengre enn å gjøre en ren kost- nytteanalyse, det handler om risiko og konsekvenser på et overordnet nivå. Terje Aven (2015) skriver at «beslutningsgrunnlaget må gjennomgås og vurderes av beslutningstaker før beslutning tas» (Aven, 2015). I neste kapittel drøftes et annet funn fra den komparative analysen, denne gangen handler det om beslutningen om å ikke opprette noe kontakt med angriperne.

Suksessfaktor 7: Ikke opprettet kontakt med angriperne

Samtlige av ofrene i denne studien har forklart at de opprettet aldri kontakt med angriperne. Det til tross for at alle, i form av skriftlige trusselbrev, fikk instrukser om å ta kontakt eller etablere en forhandling med angriperne. Å ikke gå i dialog eller innlede forhandling ble besluttet nært i tid etter at angrepene ble kjent, ikke mer enn et par dager og gjerne tidligere også, i de ulike beslutningsgruppene. Om vi ser mer systematisk på når virksomhetene besluttet å ikke ta kontakt med angriperne, var dette sammenfallende. Men forskjellene på hvor lenge angrepet hadde pågått (angriperne var på innsiden av datasystemet) var forskjellig.

Hydro: angrepet skjedde natt til 19. mars 2019, angriperne hadde vært inne siden desember året før).
Inocean: Angriperne hadde vært inne i flere måneder.
Østre Toten: Har ikke en klar oversikt, opplyser i intervju at det kan være snakk om uker.
Amedia: Angriperne kom inn få dager før.
Stangeland Maskin: Har ikke en klar oversikt, besluttet under en uke etter angrepet at de skulle bygge hele datasystemene på nytt.

Som vi så i teorikapittelet er frykt (Chen, 2016) funnet å være en kraftig emosjonell respons på en oppfattet trussel. Frykt påvirker menneskelig atferd direkte og kan fungere som en motivator for mennesker til å endre sin normale atferd for å avverge et potensielt negativt utfall (ibid). Fryktet ofrene i denne studien angriperne? Kjente de på redsel for å ta kontakt med trusselaktørene? Var det derfor de unnlot å opprette kontakt? Eller var det fordi de tidlig kjente på en fortrolighet i forhold til å løse saken uten å innlede kontakt med de datakriminelle? Selskapet med færrest ansatte i studien er ingeniørselskapet Inocean som driver med avansert havvind teknologi. Selskapet ble frastjålet verdifulle tegninger og annen dokumentasjon. Inocean har forklart i intervjuene hvordan angrepet kom overraskende og uventet og hvordan angriperne distribuerte et trusselbrev om hvilke data som var stjålet via de ansattes Teams-kontoer. Inocean har i samme intervju uttrykt at det var tidskritisk for dem å komme tilbake til normalen, men det var ikke aktuelt å opprette kontakt med de kriminelle angriperne. Samme virksomhet har beskrevet den første perioden da angrepet skjedde, hvordan denne perioden var preget av kaos og at ingen av dem som var satt til å løse saken hadde personlig erfaring eller hadde opplevd å være en del av et omfattende dataangrep før.

Daniel Kahneman (2012) beskriver det han omtaler som system 1 og system 2 når det kommer til beslutningsprosesser. Kort oppsummert virker system 1 automatisk, intuitivt og hurtig, system 2 står for de mer anstrengende mentale aktivitetene. Systemet sammenfaller med det Engen med flere (2016) omtaler som intuitive og analytiske beslutninger. For å dukke videre i dette beskriver Kahneman faren med det han omtaler som «Priming»-effekt, hvordan assosiasjoner og gjenkjennelse av situasjoner kan bidrar til senket årvåkenhet og kritisk gjennomgang når valg og beslutninger skal fattes.(Kahneman 2012 s. 66 - 67).

Kan en del av forklaringen for at ingen ofrene i denne studien opprettet kontakt med angriperne var at de var helt uten tidligere erfaring om løsepengevirus og derav var det ikke var mulig å «hoppe» til konklusjoner og assosiasjoner? Beslutningstakerne måtte gjennom «System 2» prosessene for å virkelig i dybden analysere og kritisk vurdere sine valg og beslutninger, var det på den måten virksomhetene kom frem til suksessfaktorene som til sammen skulle vise seg å bli løsningen på en utfordrende og kritisk situasjon?

Informanten fra Hydro er inne på noe helt sentralt når han forklarer hvordan Hydro i 2019 jobbet for å løse situasjonen de sto i;

- *For oss var det viktig å skynde seg langsomt.*

På denne måten kommuniserer informanten fra Hydro to ting, saken var tidskritisk, men samtidig var det viktig for virksomhetene å finne tid og nøye vurdere og analysere de skrittene mot en endelig løsning. Igjen i sitatet finner vi ytterpunktene mellom Kahnemans System 1 og System 2, intuitive og analytiske beslutningstaking samt Eid og Johnsens (2018) system for hvordan beslutninger blir til.

Suksessfaktor 8: Eksterne bidragsytere

Krisehåndtering innebærer å ta vanskelige valg. Ofrene som er intervjuet i denne studien har alle benyttet eksterne bidragsytere i form av ekspertise. Ikke noen av informantene hadde, verken personlig eller blant andre de andre deltakerne i beslutningsgruppen, personlig erfaring med dataangrep fra før. Det er store likheter med forskningen i teorien og det informantene sier. Spesielt kommer dette til uttrykk i sitatene om

Ofrene i denne studien har i sum ikke engang opprettet kontakt med angriperne, de har i tillegg oversett truslene fra angriperne og kontaktet ekstern hjelp, anmeldt saken til politiet og bedt om assistanse fra nasjonale ressurser i form av Datatilsynet eller Nasjonal Sikkerhetsmyndighet (NSM). I sum har trusselbrevene fra angruperne alle kommunisert at det å kontakte myndigheter eller å be om hjelp kunne medføre konsekvenser, enten i form av at løsepengesummen ville bli høyere eller at en ble eksponert på «shaminglister» på det

mørke nettet, eller som Stangeland Maskin fikk beskjed om: «Uteblir betaling vil vi angripe dere igjen».

Ingen av informantene sier at de angrer på at de ba om hjelp, alle setter ord på at det har vært et viktig bidrag for å løse saken. Ekspertenes bidrag beskrives å inneholde alt fra at de hadde viktig kunnskap og kunne dele fakta om dataangrep og løsepenger, at de fremsto dyktige og løsningsorienterte, at de hadde teknisk kunnskap om hvordan virksomhetene skulle stenge ned og av datasystemene for å hindre nye angrep, hvordan en skulle få systemene «opp å gå igjen» osv.

Som vi var inne på i teorikapittelet innebærer krisehåndtering å ta vanskelige valg. Rosenthal, Charles og ’t Hart (1998) viser i sin definisjon hva en krise er, «En alvorlig trussel mot strukturer, verdier og normer i et sosialt system som under tidspress og usikkerhet gjør det nødvendig å foreta kritiske beslutninger» at det handler om å ta beslutninger i et miljø med trussel, hastverk og usikkerhet og at behovet for å redusere usikkerhet og å mestre krisens kompleksitet krever innspill av ekspertrådgivere i en beslutningsprosess. (Rosenthal, Charles og ’t Hart, 1998, s. 10). Som vi ser fra Rosenthal, Charles og ’t Hart er det nøyaktig det som informantene beskriver har skjedd. Det er også slik de har opplevd at støtten og tilstedeværelsen fra ekspertene har fungert.

Men kriser medfører stor belastning både for beslutningstakerne og ekspertene, argumenterer Rosenthal, Charles og ’t Hart (1998). De advarer mot at psykologiske biaser som «gunstig tolkning av data» eller «tunnelsyn» kan oppstå, og at for å unngå biaser må ekspertene og beslutningstakerne utvikle en forståelse for hverandres roller i beslutningsprosessen. Sagt med andre ord kan en kanskje lett la seg begeistre når ekspertene kommer med sin unike kunnskap om et fenomen og skal i gang med å ordne opp i saken. Begeistring for ekspertenes bidrag finner en også i denne studien:

- *Vi hadde aldri klart det uten dem*
- *Deres bidrag var helt avgjørende for at vi klarte å etablere en tidslinje for når angriperne kom inn*

- *Firmaet vi leide inn visste hva de skulle gjøre. Det var de som greide å spore seg tilbake og finne ut når de (angriperne) kom seg inn i systemene våre.*

I forbindelse med analysene som er gjort av intervjuene finner jeg at oppdragene som de eksterne hjelperne, eller ekspertene, har hatt i denne saken, alle har vært konkrete og avklarte. Saken det er bedt om bistand for å løse har fremstått som kaotisk for ofrene, men oppgavene ekspertene fikk i disse sakene fremstår som mer presise og avklarte, en må huske på at mens Amedia var avskåret for delvis å gi ut papiraviser og utbetale lønn var det en stor krise for dem, men det var ikke den saken ekspertene var satt til å løse. Deres oppdrag var å bistå med å løse løsepengeviruset. Det blir feil å beskrive oppdraget ekspertene fikk som enkelt, det er ikke hensikten, hensikten er å sette oppdragene og situasjonen inn i den situasjonen som var den reelle tilstanden den gangen og se på sakens fakta i lys av det som informantene har beskrevet skjedde. Samtlige av informantene i denne studien valgte å overse kravet fra trusselaktørene, be om ekstern bistand, anmelde til ansvarlige myndigheter og samtlige melder at det gikk bra.

Suksessfaktor 9: Menneskene bak: Å motivere

Når leder skal lede gjennom en krise har det gjennom denne studien kommet tydelig frem at en suksessfaktor virksomhetene har omtalt er verdien av å motivere arbeidsteamet (beslutningsgruppen), og hvor viktig motivasjon har vært for å oppnå resultat.

Informanten fra Stangeland Maskin uttrykker det slik:

Men suksessen bak historien er mennesker som jobber med det etterpå, vi er jo avhengige av å engasjere de som er der, vårt mandat er: Hvordan kan vi motivere?

Men hva ligger egentlig i det å skulle motivere, og hvorfor fremstår det som viktig i en sak om å løse et løsepengevirus?

Vi vender oss til teoridelen og trekker inn hva Eid og Johnsen (2018) skriver om motivasjon. Motivasjon kan forstås som indre prosesser som påvirker retning og styrke på menneskelig atferd og mål (Eid & Johnsen, 2018, s. 119 - 120). Forfatterne viste til Maslows behovspyramide for å forstå hva som motiverer menneskelig motivasjon. Forfatterne beskriver at modellen kan relateres til operative tjenester og at ledere, ved å ha innsikt i hva

som motiverer, kan oppnå prestasjoner gjennom nettopp å motivere. Maslows behovspyramide beskriver anerkjennelse som et viktig element. Kombinasjonen av å motivere og det å vite hva det er som motiverer kommer også til uttrykk gjennom denne studien, en informant beskriver det slik;

«*Skal vi peke på en ting som er den virkelige suksessen bak denne historien er det menneskene som jobbet med å løse saken».*

En av suksessfaktorene som fremstår som avgjørende for å løse et løsepengevirus med potensielt alvorlige konsekvenser er altså å motivere arbeidsgruppen (beslutningstakere) og på den måten komme i mål.

Fra nå å ha drøftet faktorene som i denne komparative studien er identifisert som suksessfaktorene for å løse et løsepengevirus er det er viktig å understreker at nummereringen av suksessfaktorene ikke er uttrykk for en kronologisk rekkefølge. Det er ikke slik at den ene faktoren som er listet opp som nummer en og to osv er viktigere enn den andre, det er summen av faktorene til sammen som medførte at virksomhetene løste krisen.

En går herfra videre for å diskutere suksessfaktorene i stort. Det er for å sette faktorene i et kritisk lys og for å på den måten kunne komme nærmere og gi svar på det som er hele denne studiens utgangspunkt, en problemstilling som etterspør; **Hvilke faktorer bidro til en suksessfull håndtering av betalingskravet et løsepengevirus medfører?**

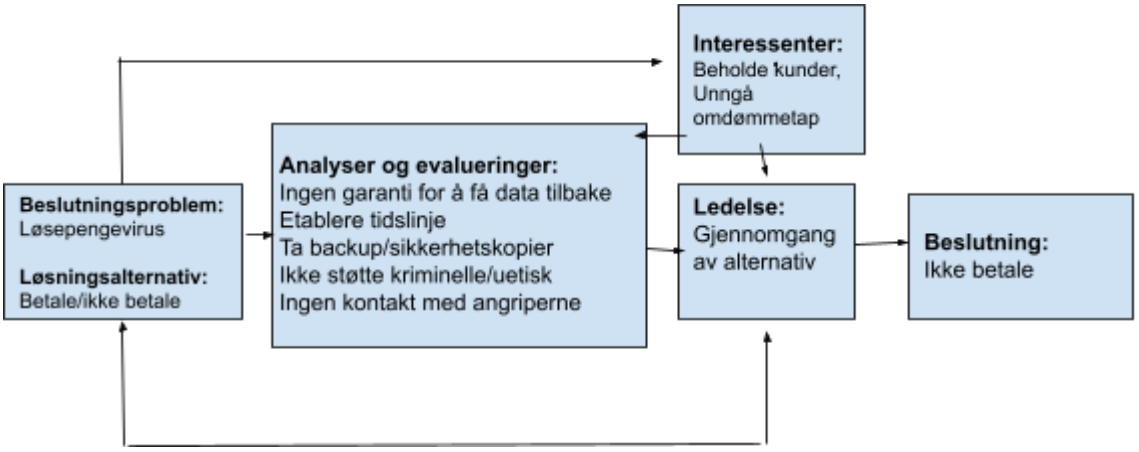
5.2 Drøfting av problemstillingen i sin helhet

Hvilke faktorer skal til for å få til en god risikostyring? Og hvilke faktorer var det som ga grunnlag for best mulig beslutningsstøtte for å løse virksomhetenes betalingsdilemma? Sagt med andre ord: Var det en god beslutning å ikke betale løsepengekravet? Det er det overordnede spørsmålet for denne drøftingsdelen.

Terje Aven (2015) skriver at for å vurdere om en beslutning var god eller ikke, må en «fokusere på prosessen forut for beslutningen, det vil si på de overveielsene og de handlingene vi foretar før beslutningen blir fattet» (Aven, 2015, s. 7).

Videre i denne drøftingsdelen er målet å gå systematisk gjennom rammeverket Aven foreslår for en slik analyse. Beslutningene som ble tatt utdypes med å trekke inn Daniel Kahnemans () teori om System 1 og System 2 om hvordan menneskehjernen jobber og fungerer når beslutninger tas.

I teoridelen ble det beskrevet hvilke elementer Aven (2015) anbefaler at inngår i en beslutningsprosess. Jeg har gjort modellen til Aven (2015) til min egen ved å legge inn empiriske funn:



Figur 1.11 Modell for beslutningstaking under usikkerhet for løsepengevirus.

For å eksemplifisere modellen brukes caset Østre Toten kommune. Kommunen opplevde at hele den kommunale tjenesteleveransen med få unntak ble rammet. I tillegg ble kommunens databaser tappet for store mengder data, i disse dataene fantes alt fra personnavn, helseopplysninger og personnummer til kommunens innbyggere. Kunne en løsning vært å betale? Kunne utfallet ha vært, at om kommunen hadde gått i forhandlinger med angriperne, kunne spredning av persondata vært unngått? I stedet valgte kommunen å ikke betale, og dermed gjennomførte trusselaktørene sine trusler, og data ble lekket. (Wilberg & Børve, KPMG, 2021, s. 8 - 9). Hvilke argumenter ble avgjørende for å ikke betale? Det er et viktig poeng å trekke inn her hva ofrene gjengir fra intervjuene om beslutningene om ikke å betale:

- *Ikke etisk riktig.*
- *Vi kunne betalt, men det finnes ingen garanti.*

I tilfellet Østre Toten kommune kunne en sett for seg et scenario der en forhandling ble inngått og en sum om løsepenger ble forhandlet frem, kommunen hadde i sitt øverste politiske organ sammen med beslutningstakere fra administrasjonen besluttet å betale for å få tilbake data. Men så hadde utfallet vært at angriperne likevel hadde omsatt de stjålne persondataene på det mørke nettet, og kanskje ikke noensinne returnert dekrypteringsnøkkel for at kommunen kunne få tilgang tilbake. Det begynner med et beslutningsproblem som i dette tilfellet er et løsepengevirus, derfra blir det gjort analyser og evalueringer.

Som vi så i teorikapittelet om safety og security (Jore, 2017) er selve definisjonsforskjellen mellom disse to ytterpunktene innslaget av onde hensikter og ikke onde hensikter. Situasjonen ofrene har måttet håndtere har alle vært initiert av aktører som med vilje og overlegg har planlagt et angrep hvor hensikten har vært å true, skade og fremkalle frykt som derav skulle utløse betaling. Betalingsdilemmaet har i så måte dreid seg om å håndtere en situasjon hvor selve hensikten har vært ond. I en slik sak, forklarer ofrene, hvor du ikke engang vet hvem som angriper deg, du vet ikke hvem motparten er, er usikkerheten enda større.

Ofrene i denne studien har i sum ikke engang opprettet kontakt med angriperne, de har i stedet unisont valgt å overse angriperens henvendelse om å innlede en forhandling, de har i sum også alle kontaktet ekstern hjelp, anmeldt saken til politiet og bedt om assistanse fra nasjonale ressurser i form av Datatilsynet eller Nasjonal Sikkerhetsmyndighet (NSM).

I skjæringspunktet mellom å betale eller ikke betale fremstår faktoren «ingen garanti» som en av de viktigste og kanskje den mest avgjørende beslutningen. Dette handler om risiko og spesielt om usikkerheten. Fra teorikapittelet ble det vist at usikkerhet er en avgjørende faktor som risikovurderinger må ta hensyn til (Aven, 2010). Samtlige av informantene i denne studien sto overfor betydelig usikkerhet da de skulle beslutte hvordan de skulle håndtere situasjonen. Fra teorien så vi at jo svakere kunnskap en har, til større blir usikkerheten om hva som kan skje (ibid). For å illustrere den betydelige usikkerheten og størrelsen av denne kan vi nevne:

Virksomhetene hadde ingen kostnadskontroll, de visste ikke hvem angriperne var,

det var usikkert når de kunne være tilbake i normal drift, de kjente ikke omfanget av angrepet, det var usikkerhet om skadeomfanget for tredjepart (personer kompromittert av angrepet) og usikkerhet om en hadde sikkerhetskopier da en besluttet å ikke betale.

Aven med flere (2008) skriver at «Risikostyring innebærer beslutningstaking i situasjoner med høy risiko og store usikkerheter, og slik beslutningstaking er utfordrende, da det er vanskelig å forutsi (predikere) konsekvensene (utfallene) av beslutningene (Aven et al, 2008, s. 21). Utfordringen for virksomhetene var at konsekvensene var store. Aven (2015) fremholder at «I situasjoner med høy risiko er det et sprang fra beslutningsunderlaget til selve beslutningen» (Aven et al, 2008, s. 23), videre må underlaget vurderes (ibid). I den empiriske gjennomgangen av virksomhetene som betalte kom det frem at de fleste benyttet kost-nytte-analyser (KN) som beslutningsgrunnlag. Også "mannen i vinduet" fortalte at det var "enten eller" for hans virksomhet da de besluttet å betale pengekravet. De undersøkte virksomhetene i min studie inkluderte langt flere elementer i sine vurderinger i beslutningen om hvordan pengekravet skulle vurderes. Også Aven (2015) peker på at mange ser på slike analyser som «det riktige redskapet for å prioritere og velge blant løsninger" (Aven, 2015, s. 165), men understreker at «en slik tenkning holder ikke" (ibid).

Modellen for løsepengevirus på side 86 illustrerer veien frem til en beslutning hvor utgangspunktet er et beslutningsproblem. Her må det velges mellom ulike alternativer for å nå ulike krav og mål. Aven (2015) trekker frem at veien til å oppnå suksess handler om å se helheten i problemstillingen. Aven problematiserer dette, han sier at en årsak til at det oppstår mangelfull forståelse av helheten, både blant analytikere og andre fagpersoner, fører ofte til at usikkerhetsvurderingene blir mangelfulle. Utfordringen, skriver Aven, blir å presentere usikkerheter på en hensiktsmessig måte» (Aven (2015, s. 163).

I drøftingsdelen forut for denne bolken så jeg på usikkerhet og hvordan virksomhetene jobbet for å skaffe mer informasjon, forsøkte å minske usikkerhet og hvordan denne fremgangsmåten traff rammeverket til Lipsitz og Strauss (1997). Om vi går tilbake til Avens modell om beslutningstaking kan vi dykke videre ned i relevant teori om det å skulle beslutte og hva som påvirker en beslutningsprosess.

Daniel Kahneman (2012) og Engen med flere (2016) gjør et skille mellom system 1 og system 2 (Kahneman 2012) og intuitive og analytiske vurderinger (Engen et al, 2016). De to systemene handler om hvordan mennesker fatter beslutninger og hvordan samspillet mellom det å raskt vurdere - eller mer analytisk vurdere konsekvenser og utfall av en situasjon. Kahneman påpeker at det er flere faktorer som påvirker beslutningsevnen. Vi finner igjen eksempler på dette i sakene om løsepengevirusene. Vi kan ta for oss den første situasjonen som oppsto, den gangen da de første meldingene om løsepengevirusene ble kjent.

Samtlige informantene har forklart at det fantes lite kunnskap om situasjonen de sto ovenfor, og selv om et trusselbrev informerte hvordan virksomhetene kunne komme tilbake til normalen - om de betalte - var det ingen av ofrene i denne studien som gjorde det. Kahneman (2012) forklarer hvordan hjernen ved bruk av system 1 raskt og automatisk og med liten eller ingen anstrengelse finner løsninger, dette systemet leverer en strøm av inntrykk og følelser. Her kan nevnes «priming-effekten» som handler om hvordan assosiasjoner bidrar til å skape en «kognitiv letthet». Kan hende angriperne med sine trusselbrev ønsker å oppnå nettopp en slik effekt ved å tilby en «løsning» gjennom trusselbrevene som kan fremstå som en «quick-fix» på problemet. Kahneman beskriver at menneskehjernen vil lete etter sammenhenger når en situasjon oppstår. Vil situasjonene man står foran mest sannsynlig gå bra, eller kan det ende med en ulykke? I intervjuene forklarte alle ofrene om en krevende situasjon - men som hadde et positivt utfall i form av at en unngikk å betale pengekravet. Utover det måtte virksomhetene løse en situasjon som både var omfattende og alvorlig og preget av stor usikkerhet. Ingen av informantene hadde personlig erfaring med tilsvarende hendelse før, men kun lest eller hørt om løsepengevirus og forbandt saken med noe som var alvorlig og omfattende.

Kahneman (2012) beskriver videre at priming begrenser seg ikke bare til begreper eller ord, men kan inkludere så vel hendelser, synsinntrykk, bilder etc. Vi så innledningsvis i forskningen om «de som betalte», at skam, skyldfølelse, frykt for omdømmetap osv var grunner ofrene oppga **for** å betale. Ofrene veide også kostnadene opp mot fordeler før de besluttet å betale. Mei-Fang Chen viser i sin forskning at frykt er en sterk motivator for mennesker til å endre sin normale atferd for å avverge et potensielt negativt utfall (Chen, 2016). Men hva avgjør hva mennesker opplever er et negativt utfall? Aven med flere (2004) beskriver hvordan oppfattelse og håndtering av farer kan oppleves og håndteres ulikt ut fra

den enkeltes risikopersepsjon. Eid og Johnsen (2018) skriver at selve forutsetningen for å forstå atferd i operasjonelle sammenhenger er at «individets oppmerksomhet er imidlertid avgjørende for evnen til informasjonsbehandling og beslutningstaking i operative situasjoner» (Eid & Johnsen, 2018; s.). Det er vanskelig å vurdere på hvilken måte og hvordan ofrenes risikopersepsjon medvirket i studien om de som betalte, men i denne studien, kan en se at informantene opplevde at løsepengeviruset utgjorde en trussel for virksomheten og at det ble tatt flere grep før en besluttet å ikke betale.

Et annet moment som er verdt å kritisk diskutere er om det er ofrenes økonomiske situasjon som var årsaken til at en klarte å håndtere løsepengeviruset uten å betale. Som vi så i fra den internasjonale studien om dem som betalte var faktorene skam og frykt en stor del av årsaken til at anerkjente institusjoner faktisk betalte. Hvorfor kjente ikke våre informanter på samme faktorer? Var det fordi de ikke ønsket å opplyse om det i intervjuene, eller var det fordi de faktisk ikke kjente på slike følelser? Vi kan se på ingeniørselskapet Inocean og hva de argumenterer med når det kommer til hvorfor de ikke betalte:

- Det var at vi skulle ikke gi dem noe som helst påskudd til at dette er business. Vi skal ikke feige ut. Dette her skal vi klare.

I sitatet kommer det klart frem at det var lagvilje og ståpåvilje i teamet til Inocean som var med på å definere hva som var medvirkende til at en ikke ville betale. Inocean er ikke et stort konsern med flere tusen ansatte, men et nyere og mindre teknologiselskap. Selskapet oppgir å ha 25 faste ansatte, stiftet i 1996. Selskapet hadde ingen økonomisk eier i ryggen som grep inn og garanterte for virksomhetens økonomi da datasystemet lå nede og skjermene var svarte. Overføringsverdien til andre virksomheter fra denne studiens funn er forsøkt å favne bredt i form av hvilke virksomheter som er utvalgt og hvilke historier de har å fortelle. Undersøkelsen handler både om privat og offentlig virksomhet, men også det «lille» firmaet med 25 ansatte som likevel, til tross for hva de sto i, klarte å lande en vanskelig og komplisert sak.

Vi ser gjennom intervjuene og den komparative analysen av casene at Inocean har handlet akkurat likt og tatt de samme vurderingene som «de store». Jeg vender tilbake til Inocean og

funnene fra denne studien i det neste drøftingssporet i denne oppgaven. Det handler om faktorenes overføringsverdi til andre virksomheter.

5.3 Faktorenes overføringsverdi til andre virksomheter

Kan andre virksomheter og beslutningstakerer nyttiggjøre funn fra denne studien, eller er funnene av en slik karakter at de er så særegne og unike for virksomhetene som er studert at de for andre vil fremstå for krevende å «kopiere»?

På den andre siden er det viktig å huske at sikkerhet aldri kan bli statisk, alt som skjer innen det digitale er dynamiske prosesser. I tilfellet løsepengevirus handler det om ondsinnede handlinger der angripernes motivasjon utelukkende er igangsatt for å oppnå økonomisk gevinst ved å spre frykt og skade. Slik kriminell virksomhet har potensial til å medføre alvorlige skadelige konsekvenser for samfunnet.

Det bør i denne delen av oppgaven også diskuteres om det er slik at det kun vil være ressurssterke og store virksomheter med sterk økonomi som vil klare å håndtere et løsepengevirus uten å betale. Store konsern som Amedia og Hydro er ressurssterke virksomheter med god økonomi, men hva med frisøren på gatehjørnet eller en mellomstor bedrift, som bedriften til mannen i Ostehuset, kunne han brukt samme «oppskrift»? Det er vanskelig å svare sikkert på et slikt spørsmål, som vi så i studien om «de som betalte» var mye av argumentasjonen for å betale at virksomhetene gjennomførte kost-nytte analyser og ut fra det vurderte at det ville koste mindre å betale angriperne, få data i retur og unngå skam, omdømmetap og merarbeid med å gjenopprette data. Denne studien dokumenterer at virksomhetene gjorde langt mer enn rene kost- nytteanalyse før de bestemte seg for hvordan de håndtere betalingskravet.

Anbefalt videre forskning

Jeg anbefaler at det forskes mer på betaling og løsepengevirus. Siden det er et stort problem at mange betaler, er det viktig å komme nærmere hvordan samfunnet kan komme til bunns i disse krevende og uoversiktlige sakene. Det kan best møtes med kunnskapsbasert forskning og fakta på bordet.

6.0 Konklusjon

Det europeiske byrået for nettverks- og informasjonssikkerhet, ENISA, har siden 2021 rangert løsepengevirus som den største digitale trusselen over hele EU. Samme byrå anslår at over seksti prosent av ofrene betaler store penger til kriminelle hackere for å få data tilbake. Også norske virksomheter rammes, alt fra store private selskaper til offentlige norske institusjoner, har opplevd produksjonsstopp og omfattende systemlammelser som følge av løsepengevirusene.

Et komparativt casestudie av fem virksomheter, supplert med en dokumentanalyse, viser hvilke faktorer som var avgjørende for at verken Amedia, Hydro, Inocean, Stangeland Maskin eller Østre Toten kommune betalte løsepenger da de ble krevd store beløp etter løsepengevirus-angrep. Studien dokumenterer følgende ni sammenfallende faktorer: Først var det nødvendig å reagere akutt og etablere en egen krisestab. Det var viktig fordi en slik erkjente risikoen og systematiserte et forsvar for å håndtere krisen. Faktor to handler om ledelsens støtte, det var viktig for å kunne kjenne på trygghet og tilføre motivasjon og støtte.

Suksessfaktor nummer tre var å fatte beslutninger under stor usikkerhet, det var nødvendig for skulle de vente til all sikker kunnskap var på bordet, kunne de kanskje ventet fortsatt. Den fjerde faktoren var forsøket på å etablere en tidslinje, det var viktig for å undersøke hvor lenge de digitale innbruddene hadde pågått. Faktor nummer fem var at en ikke ønsket å støtte kriminelle, nummer seks var at betaling i seg selv ikke medførte noen garanti for å få igjen data. Den sjuende suksessfaktoren var å ignorere angriperne ved å ikke opprette kontakt, den åttende suksessfaktoren var ekstern støtte, det var viktig for å få dedikert hjelp. Den siste faktoren handlet om at menneskene støttet og motiverte hverandre, det var viktig for fellesskapsfølelsen og motivasjonen når nettene ble lange og krisen vedvarte. Faktorene til sammen viser at det måtte langt større virkemidler til enn en isolert kost-nytte analyse for å fatte beslutning om en skulle betale - eller ikke betale - kriminelle hackere.

7.0 Referanser

Andersen, S. S. (2006). Aktiv informantintervjuing, Universitetsforlaget.

Andersen, S. S. (2013). Casestudier. Forskningsstrategi, generalisering og forklaring (2. utg.). Oslo: Fagbokforlaget

Amundrud, Ø., & Aven, T. (2015). On how to understand and acknowledge risk. Reliability Engineering and System Safety, 42-47.

Aven, T. (2015). Risikostyring (2. utg) Universitetsforlaget.

Aven, T., & Renn, O. (2010). Risk Management and Governance. Concepts, Guidelines and Applications. Berlin: Springer.

Aven, T., Røed, W., Wiencke, H.S. (2008). Risikoanalyse. Universitetsforlaget

Aven, T., Boyesen, M., Njå, O., Olsen, K. H., & Sandve, K (2004). (7 utg.). Samfunnssikkerhet. Oslo: Universitetsforlaget.

Beck, U. 1997. Risiko og Frihet. Norsk utgave. Fagbokforlaget Vigmostad og Bjørke AS, Sandviken, Bergen.

Bergsjø, H., Windvik, R. & Øverlier, L. (2020). Digital sikkerhet – en innføring. Universitetsforlaget.

Brantly, A. F. (2014) 'The cyber losers', Democracy and Security, vol. 10, nei. 2, s. 132-55

Bruun, F. & Vatne, D. (1990) Organisasjonslære. Universitetsforlaget

Chen, M. F. (2016) Impact of fear appeals on pro-environmental behavior and crucial determinants. International Journal of Advertising, 35:1, 74-92, DOI: 10.1080/02650487.2015.1101908

Collins, A. & Baccarini, D. (2004). Project success - A survey. Journal of Construction Research. 5. 211-231. 10.1142/S1609945104000152.

Connolly, A. Y & Borrion, H. (2022) Reducing Ransomware Crime: Analysis of Victims' Payment Decisions, Computers & Security, Volume 119, 2022, ISSN 0167-4048.

Dalen, M. (2004). Intervju som forskningsmetode : en kvalitativ tilnærming (p. 136). Universitetsforl.

Engen, O. A. H., Kruke, Bjørn I, Lindøe, Preben Hempel Lindøe , Olsen, Kjell Harald , Olsen, Odd Einar og Pettersen, Kenneth Arne. (2021). Perspektiver på samfunnssikkerhet. Cappelen Damm. Oslo.

Engen, O. A, H., Kruke, Bjørn I., Lindøe, Preben Hempel Lindøe , Olsen, Kjell Harald , Olsen, Odd Einar og Pettersen, Kenneth Arne. (2016). Perspektiver på samfunnssikkerhet. Cappelen Damm. Oslo.

Eid, J. & Johnsen, B. H. (2018). Operativ psykologi (3 utg.). Bergen: Fagbokforlaget

Flin, R. H., O'Connor, P., & Crichton, M. (2008). Safety at the sharp end: A guide to non-technical skills. Aldershot, UK: Ashgate Publishing.

Flyvbjerg, B. (2004). Five Misunderstandings About Case-Study Research. Qualitative Inquiry, 12(2), 219–245. https://doi.org/10.1177/1077800405284363

Garborg, A. (1918). «Fyreord» i Homer: Odyssevskvædet, oversatt av Arne Garborg. Kristiania: H. Aschehoug & Co.

Halvorsen, K. (2008). Å forske på samfunnet: en innføring i samfunnsvitenskapelig metode. Oslo: Cappelen akademisk forlag

Hauben, M. (2007). History of ARPANET. Site de l'Instituto Superior de Engenharia do Porto, 17.

Johannessen, A., Christoffersen, L., & Tufte, P. A. (2021). *Introduksjon til samfunnsvitenskapelig metode* (6. utgave.). Abstrakt forlag.

Johnston, Allen C. & Warkentin, Merrill. 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly*, (34: 3) pp.549-566.

Jore, S. (2017). The Conceptual and Scientific Demarcation of Security in Contrast to Safety. European Journal for Security Research, 4(1), 157–174.

Kahneman, D. (2012) Tenk fort og langsomt. Oslo: Pax forlag

Kjellen, U., & Albrechtsen, E. (2017). Prevention of Accidents and Unwanted Occurrences: Theory, Methods, and Tools in Safety Management, Second Edition (2nd ed.). CRC Press.

Kvale, S. og Brinkmann, S. (2018) Det kvalitative forskningsintervju Oslo: Gyldendal Norsk Forlag

Kruke, B.I. (2015). Planning for crisis response. The case of the population contribution, i L. Podofillini, B. Sudret, B. Stojadinovic, E. Zio og W. Kröger (red.) Safety and reliability of complex engineered systems. ESREL. London: CRC Press.

Kydland, F. E., & Prescott, E. C. (1977) Rules Rather than Discretion: The Inconsistency of Optimal Plans. Journal of Political Economy, 85 (3), 473–491. http://www.jstor.org/stable/1830193

Larsen, A. K., (2007) En enklere metode: Veiledning i samfunnsvitenskapelig forskningsmetode Fagbokforlaget

Lincoln, Y. S., & Guba, E. G. (1985). Naturalistic inquiry. Sage.

Lipshitz, R., Klein, G., Orasanu, J., & Salas, E. (2001). Focus article: Taking stock of naturalistic decision making. Journal of Behavioral Decision Making, 14, 331-352

Lipshitz, R., Strauss, O. (1997) Coping with Uncertainty: A Naturalistic Decision - Making Analysis.

Martin, P. (2019) Rules of Security Staying Safe in a Risky World Oxford University Press

Malterud, K. (2017). Kvalitative metoder i medisinsk forskning: en innføring. Oslo: Tano Aschehoug.

Maxwell, J. A. (2009) Designing Qualitative Study. In L. Bickman & D.J Rog (Red). The 123 SAGE Handbook of Applied Social Research Methods (s. 214 - 250). London: Sage

Mehmetoglu, M. (2004). *Kvalitativ metode for merkantile fag*. Fagbokforlaget

Mellon, C, Bergen, P. Sterman, D. (2017) To pay ransom or not to pay ransom? An Examination of Western Hostage Policies. New America International Security Policy Paper. https://d1y8sb8igg2f8e.cloudfront.net/documents/hostage-paper-final.pdf

Rausand, M. Utne, B. I. (2009): Risikoanalyse - teorier og metoder. Fagbokforlaget.

Renaud, K. Orgeron, C., Warkentin, M. & French, P. (2020). Cyber Security Responsibilization: An Evaluation of the Intervention Approaches Adopted by the Five Eyes Countries and China. Public Administration Review. 80. (4), s. 577–589.

Renn, O. (2008). Risk governance: coping with uncertainty in a complex world. Earthscan.

Rosenthal, U. (2001). Managing crises: Threats, dilemmas, opportunities. Springfield (Ill.): Thomas.

Rosenthal U. Charles M. T. & Hart P. 't. (1989). Coping with crises: the management of disasters, riots and terrorism. C.C. Thomas.

Rosenthal, U. Hart, Paul't (1991) Experts and Decision Makers in Crisis Situations SAGE Publications https://doi.org/10.1177/107554709101200402

Silkoset, Gripsrud, G., & Olsson, U. H. (2021). *Metode, dataanalyse og innsikt* (4. utgave.). Cappelen Damm akademisk

Tjora, A. H. (2021). Kvalitative forskningsmetoder i praksis (4. utgave.). Gyldendal.

Trochim, W. M. (1989). Outcome pattern matching and program theory. *Evaluation and program planning*, *12*(4), 355-366.

Weimann, G. (2016) Going Dark: Terrorism on the Dark Web, Studies in Conflict & Terrorism

Xavier, U.H., & Pati, B.P. (2012). Study of internet security threats among home users. Fourth International Conference on Computational Aspects of Social Networks (CASoN), 217-221.

Yar, M. og Steinmetz, K.F. (2019) Cybercrime and Society. 3. utg. Sage Publications.

Yin, R.K. (2015) Case Study Research: Design and Methods 5. edition SAGE Publications

Yin, R. K. (2018) Case Study Research and Applications Design and Methods 6. edition SAGE

Young, A.L., & Yung, M. (1996). Cryptovirology: extortion-based security threats and countermeasures. Proceedings 1996 IEEE Symposium on Security and Privacy, 129-140.

Østbø L. V. (2021) Cyberkriminalitet mot næringslivet: en studie av løsepengevirusangrep mot norske virksomheter [Masteroppgave, Universitetet i Oslo]. DUO Vitenarkiv. https://www.duo.uio.no/bitstream/handle/10852/89417/1/LEVERINGSKLAR.pdf

Aarset, Magne. (2010) Kriseledelse. Fagbokforlaget.

Digitale rapporter

Australian Government: Ransomware Action Plan
https://www.homeaffairs.gov.au/cyber-security-subsite/files/ransomware-action-plan.pdf

Australian Cyber Security Strategy 2023-2030
https://www.homeaffairs.gov.au/reports-and-pubs/files/2023-2030_australian_cyber_security_strategy_discussion_paper.pdf

Direktoratet for samfunnssikkerhet og beredskap, DSB (Januar 2020) *Risikostyring i digitale verdikjeder*
https://www.dsbinfo.no/DSBno/2020/rapport/risikostyring-i-digitale-verdikjeder/?page=2

ENISA (October 2021) *ENISA threat landscape 2021*
https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

ENISA (Juli 2022) *Threat landscape for ransomware attacks*
https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks

ENISA (October 2022) *ENISA threat landscape 2022*
https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Europol's European Cybercrime Centre (2017) Internet organised crime crime threat assessment
https://www.europol.europa.eu/sites/default/files/documents/iocta2017.pdf

KPMG (august 2021) *IKT-sikkerhet i Østre Toten kommune forut for dataangrepet 9. januar 2021*
https://www.ototen.no/_f/p1/i40fd2566-64fa-437b-b0e1-73cb446d3775/sikkerhetsrapport-usladdet-versjon.pdf

KPMG (Mai 2022) *IKT-sikkerhet i Østre Toten kommune forut for dataangrepet 9. januar 2021*
https://www.ototen.no/_f/p1/i40fd2566-64fa-437b-b0e1-73cb446d3775/sikkerhetsrapport-usladdet-versjon.pdf

Nasjonal Sikkerhetsmyndighet, NSM *Risiko (Oktober 2021) Nasjonalt digitalt risikobilde 2021*
https://nsm.no/aktuelt/nasjonalt-digitalt-risikobilde-2021

Nasjonal Sikkerhetsmyndighet, NSM *Risiko (Oktober 2022): Økt risiko krever økt årvåkenhet*
https://nsm.no/getfile.php/137798-1644424185/NSM/Filer/Dokumenter/Rapporter/NSM_rapport_final_online_enekeltsider.pdf

Norsk senter for informasjonssikring NorSIS. (Mai 2020) *Få en tryggere digital hverdag: Trusler og trender 2019 - 2020* https://norsis.no/content/uploads/2022/05/NorSIS_TruslerTrender_2020.pdf

Norsk senter for informasjonssikring NorSIS. (Mars 2021) *Trusler og trender 2021*
https://norsis.no/publikasjoner/

Næringslivet Sikkerhetsråds (September 2022) *Mørketallsundersøkelsen, 2022. nr. 13*
https://www.nsr-org.no/uploads/documents/Publikasjoner/Morketalls-2022-web-sider.pdf

Threat Landscape Report. (2022). ENISA: Threat Landscape Report 2022
https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Nettsider med organisasjon som forfatter

Amedia, (2022, 3. januar) Oppdatering om dataangrepet mot Amedia
https://www.amedia.no/aktuelt/dataangrep/oppdatering-om-dataangrepet-mot-amedia

Crimes Legislation Amendment (Ransomware Action Plan) Bill 2022 No. 2022 https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r6855_first-reps/toc_pdf/22025b01.pdf;fileType=application%2Fpdf

Datatilsynet. (2012, 24. januar) Informasjonssikkerhet og internkontroll: Kryptering Hentet 15. april 2023 https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/kryptering/

De nasjonale forskningsetiske komiteene. (2019, 10. februar). Generelle forskningsetiske retningslinjer https://www.forskningsetikk.no/retningslinjer/generelle/

Innstilling fra forsvarskomiteen og justiskomiteen om samfunnssikkerhet - Veien til et mindre sårbart samfunn https://www.stortinget.no/globalassets/pdf/innstillinger/stortinget/2002-2003/inns-200203-009.pdf

Nasjonal sikkerhetsmyndighet (2021, 30.06). Sikkerhetstiltak mot digital utpressing og andre angrep https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/digital-utpressing/sikkerhetstiltak-mot-digital-utpressing-og-andre-angrep

Norsk Hydro (2020, 14. Oktober). Cyberangrep på Hydro. https://www.hydro.com/noNO/media/pa-dagsorden/cyberangrep-pa-hydro/

Securityworldmarket (2020, 21. april). Ny løsepenge-taktikk: Dobbel utpressing https://www.securityworldmarket.com/no/Nyhetsarkiv/ny-losepenge-taktikk-dobbel-utpressing

Telenor: Sikkerhetsordboken https://www.telenor.no/sikkerhet/ordbok/#S

Trend Micro (2020) Annual Cybersecurity Report: *A Constant State of Flux* *https://documents.trendmicro.com/assets/rpt/rpt-a-constant-state-of-flux.pdf*

Avisartikler

Bjørkeng, P.K. (2021, 4. januar) Digital utpressing eksploderer – fordi de fleste betaler, *Aftenposten* https://www.aftenposten.no/kultur/i/7dQqzK/digital-utpressing-eksploderer-fordi-de-fleste-betaler

Eaton, C. Volz, D. (2021, 8. mai). U.S. Pipeline Cyberattack Forces Closure, *The Wall Street Journal.* https://www.wsj.com/articles/cyberattack-forces-closure-of-largest-u-s-refined-fuel-pipeline-11620479737?mod=article_inline

Eaton, C. Volz, D. (2021, 19. mai). The Wall Street Journal: Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom. *The Wall Street Journal.* https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636

Kropotov, V. Yarochkin, F (2020, 16. november) Cybercriminal 'Cloud of Logs' The Emerging Underground Business of Selling Access to Stolen Data, *Trendmicro* Cybercriminal Clouds of Logs»: The Emerging Underground Business of Selling Access to Stolen Data

L. O'Donnell, "University of Utah Pays 457K After Ransomware Attack," 2020. https://threatpost.com/university-of-utah-pays-457k-after-ransomware-attack/158564/

Nichols, S. (2019, 31. oktober) A Stranger's TV Went on Spending Spree with My Amazon Account — and Web Giant Did Nothing about It for Months. *The Register* https://www.theregister.co.uk/2019/10/31/amazon_account_hacking/

NRK. (2023, 14. februar). Fikk løsepengekrav på 50 millioner kroner https://www.nrk.no/rogaland/fikk-losepengekrav-pa-50-millioner-kroner-1.16296806

NTB, Ekroll, H. C. Kaur, C, Gjestad, R.H (2021, 28. desember) Amedia utsatt for alvorlig dataangrep – problemene er ikke løst, *Aftenposten* https://www.aftenposten.no/norge/i/mry9dp/amedia-utsatt-for-alvorlig-dataangrep-problemene-er-ikke-loest

Ording, O. Vigsnæs, M. K. Jåsund, B.K. Brekke, A. Grimeland, P. K. Rørslett, K. (2019, 19. mars). Hydro utsatt for dataangrep: – Ikke opplevd lignende, *NRK* https://www.nrk.no/norge/hydro-utsatt-for-dataangrep_-_--ikke-opplevd-lignende-1.14479736

Skille, Ø. B. Jarstad, L. (2021, 7. juli) Stort dataangrep mot norsk ingeniørselskap, *Norsk Rikskringkasting NRK* https://www.nrk.no/norge/stort-dataangrep-mot-norsk-ingeniorselskap-1.15568171

Tidy, J. (2020, 29. juni) How hackers extorted $1.14m from University of California, San Francisco. *BBC* https://www.bbc.com/news/technology-53214783

VG (2010, 25. juli) Al-Qaida: − Bortført franskmann er drept https://www.vg.no/nyheter/utenriks/i/51O01/al-qaida-bortfoert-franskmann-er-drept

Wernø, I. L. (2021, 11. januar) Angrepet av hackere – hele kommunen rammet. *VG* https://www.vg.no/nyheter/innenriks/i/M36r6K/angrepet-av-hackere-hele-kommunen-rammet

Norges offentlige utredninger (NOU)

NOU 2015: 13 (2015). *Digital sårbarhet – sikkert samfunn. Beskytte enkeltmennesker og samfunn i en digitalisert verden.* Justis- og beredskapsdepartementet. https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou201520150013000dddpdfs.pdf

NOU 2000: 24 (2000). *Et sårbart samfunn – Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet.* Justis- og beredskapsdepartementet. https://www.regjeringen.no/no/dokumenter/nou-2000-24/id143248/

Stortingsmeldinger

St.meld. nr. 17 (2001-2002) Samfunnssikkerhet Veien til et mindre sårbart samfunn https://www.regjeringen.no/contentassets/ee63e1dd1a16409fa0bb737bfda9279a/no/pdfa/stm200120020017000dddpdfa.pdf

Meld. St. 9 (2022-2023). Nasjonal kontroll og digital motstandskraft for å ivareta nasjonal sikkerhet så åpent som mulig, så sikkert som nødvendig. Justis- og beredskapsdepartementet. https://www.regjeringen.no/contentassets/d256b455415c4cae8a710f62cc97d4f9/no/pdfs/stm202220230009000dddpdfs.pdf

Andre

Australian Government Department of Home Affairs (2022, 08. desember) *Australian Cyber Security Strategy*
https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/2023-2030-australian-cyber-security-strategy

Crimes Legislation Amendment (2022) Ransomware Action Plan
https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6855

CTA (2015) Lucrative Ransomware Attacks: *Analysis of the CryptoWall Version 3 Threat*
https://www.cyberthreatalliance.org/wp-content/uploads/2018/02/cryptowall-report.pdf

Hurdalsplattformen 2021 - 2025, 2021
https://www.regjeringen.no/contentassets/cb0adb6c6fee428caa81bd5b339501b0/no/pdfs/hurdalsplattformen.pdf

Senate Bill, 2021, S6806) https://www.nysenate.gov/legislation/bills/2021/S6806.

Hydro, Årsrapport 2022
https://www.hydro.com/no-NO/investorer/reports-and-presentations/annual-reports/annual-report-2022/

Amedia, Årsrapport, 2021
https://www.amedia.no/images/dokumenter/Aarsrapport2021.pdf

Østre Toten kommune, Styringsdokument 2022
https://www.ototen.no/_f/p1/ica0647b9-0169-4fc9-9154-acbbd7b61b97/styringsdokument-2022.pdf

Vedlegg 1.

Intervjuguide

1. Hvordan ble det oppdaget at virksomheten var utsatt for et løsepengevirus?
2. Hvordan ble det oppdaget at det var et trusselbrev involvert?
3. Hvem oppdaget angrepet?
4. Hvem internt i bedriften ble i første omgang varslet om angrepet?
5. Hvordan var kravet om løsepenger formulert?
6. Hvordan ble kravet formidlet?
7. Ble det kommunisert hvor mye penger angriperne villa ha?
8. Ble det tatt kontakt med angriperne?
9. Når ble det besluttet at en ikke ville betale det angriperne ba om?
10. Hvorfor ville en ikke betale kravet om løsepenger?
11. Hadde noen blant beslutningstakerne noe erfaring med lignende hendelser?
12. Ble det tatt kontakt med ressurser utenfor bedriften for å løse saken?
13. Søkte en råd fra andre utenfor bedriften?
14. Hvordan var situasjonsforståelsen om alvoret i situasjonen?
15. Ble det slått krisealarm?
16. Når og hvordan ble dette eventuelt gjort?
17. Hørte dere mer fra angriperne etter at dere besluttet å ikke betale pengekravet? (Ble trusselen i brevet fulgt opp?)