Land	Norge
Domstol	Haugaland og Sunnhordland tingrett
Parter	Btec AS mod Nordlo Haugesund AS
Dato for afgørelse	20. juni 2025
Afgørelsestype	Dom
Status	Ukendt
Dato for publicering i domsdatabasen	1. september 2025
Omtalt i It-kontraktret, 2. udgave	Ikke omtalt
Gengivet fra	Lovdata

Haugaland og Sunnhordland tingrett - Dom - THOS-2024-65519

Instans	Haugaland og Sunnhordland tingrett – Dom
Dato	2025-06-20
Publisert	THOS-2024-65519
Stikkord	Erstatningsrett. Dataangrep. IT-sikkerhet. Cyberangrep. Force majeure. Ansvarsbegrensning. Sikkerhetskopiering. Kjøpsloven § 40.
Sammendrag	Et IT-selskap ble utsatt for et dataangrep som påvirket flere kunder. En av kundene krevde erstatning for økonomisk tap og hevdet at selskapet hadde handlet uaktsomt og brutt avtalen om sikkerhetskopiering. Retten konkluderte med at kunden var bundet av standardavtalen, som begrenset erstatningsansvaret. Retten fant at IT-selskapet hadde tilfredsstillende sikkerhetstiltak, til tross for enkelte svakheter. Selskapet ble dømt til å betale 8 280 kroner i erstatning. Kunden måtte dekke selskapets sakskostnader på 2 152 570 kroner. (Sammendrag ved Lovdata)
Saksgang	Haugaland og Sunnhordland tingrett THOS-2024-65519 (24-065519TVI-THOS/THAU).
Parter	Btec AS (advokat Bodil Kristine Høstmælingen) mot Nordlo Haugesund AS (advokat Tage Brigt Andreassen Skoghøy).
Forfatter	Tingrettsdommer Signe M. Lundegård.

Innholdsfortegnelse

Saken gjelder krav om erstatning etter at Btec AS har mistet sine data som følge av at firmaets IT-leverandør, Nordlo Haugesund AS, ble utsatt for et betydelig dataangrep.

Framstilling av saken

Btec AS, heretter omtalt som Btec, er en produksjonsbedrift innen avansert maskinering og leverer komponenter til blant annet maritim og offshore industri. Btec As ble stiftet i august 2016. De hadde i 2021 15 ansatte. Selskapet omsatte for kr 26 millioner i 2020, året før hackerangrepet. A er daglig leder og er største aksjonær i selskapet.

Nordlo Haugesund AS, heretter omtalt som Nordlo, er en IT-leverandør som tilbyr driftstjenester, herunder såkalte ASP-løsninger (Application Service Provider), hvor kundens IT-systemer og data driftes sentralt hos leverandøren. Nordlo var opprinnelig en del av Appex AS.

Appex AS var et teknologiselskap med flere forretningsområder, blant annet innen design, utvikling og IT-drift. For å skille ut IT-driftstjenestene, ble Appex Operation AS etablert som et eget selskap i desember 2019. I 2020 ble Appex Operation AS en del av Nordlo-konsernet, som er en nordisk IT-leverandør med virksomhet i flere land. Etter oppkjøpet ble Appex Operation AS omprofilert til Nordlo Haugesund AS oktober 2020. Nordlo videreførte tjenestene som Appex Operation tidligere hadde levert, inkludert ASP-løsningen til Btec.

Appex inngikk 11.02.2011 en skriftlig avtale om levering av APS- tjenester til Delta Pump AS. Dette var et selskap som var eid av familien B. Det ble da benyttet Appex sine standardavtalevilkår. Det fremgår av avtalen at leverandøren påtar seg ansvaret for drift av kundens dataprogrammer og skal gjøre disse tilgjengelige via Internett. Kunden har tilgang til support i arbeidstiden i virkedager og ut over dette blir det etablert en bakvaktstelefon. Appex garanterer 99,5 % oppetid. Det fremgår av avtalen at Appex tar sikkerhetskopier av kundens data hver virkedag. Dersom kunden ber om det, skal leverandøren tilbakekopiere angitte data fra siste sikkerhetskopi.

I pkt. 8 i avtalen fremgår det følgende:

> *Dersom Avtalens gjennomføring helt eller delvis hindres, eller i vesentlig grad vanskeliggjøres av forhold som ligger utenfor partenes kontroll, suspenderes partenes plikter i den utstrekning forholdet er relevant, og for så lang tid som forholdet varer. Slike forhold inkluderer, men er ikke begrenset til, streik, lockout, og ethvert forhold som etter norsk rett kan bli bedømt som force majeure.*

Etter pkt. 10 *kan den part som rammes krever erstatning for dokumentert økonomisk tap eller alminnelige prinsipper for erstatning i avtaleforhold. Indirekte tap dekker imidlertid ikke. Som indirekte tap regner, dog ikke begrenset til, Kundens tap av fortjeneste av enhver tap, tap grunnet driftsavbrudd, avsavnstap, samt krav fra tredjepart. Erstatningskravet etter denne bestemmelsen kan ikke overstige et beløp som tilsvarer 3 månedsleier i henhold til denne Avtalen.*

Sommeren 2011 ble Appex bedt om å etablere ASP også for Delta Maskinering. Det var samme eiere og ledelse i dette selskapet som i Delta Pump, dvs. familien B.

Delta Maskinering ble kjøpt opp av Btec i februar 2017, og hovedeier og daglig leder, A, tok over som daglig leder også i Delta Maskinering. Det ble opprettet en APS- bruker for ham i Delta Maskinering.

Det ble mellom Btec og Nordlo i mars 2017 inngått en avtale om ASP-løsning, hvor Btec fikk tilgang til sine applikasjoner og data via Nordlos servere. Det foreligger imidlertid ingen signert kontrakt mellom partene. Daglig leder i Btec, A, ba om at det ble opprettet ASP-løsninger slik han hadde hatt i Delta Maskinering. Btec ble innkalt til to møter med Appex, men møtte ikke til disse og ASP-løsningen ble tatt i bruk uten at det ble signert noen skriftlig kontrakt. Det er uenighet om hvilke vilkår som gjaldt, herunder om Nordlos standardavtale (SSA-L) med ansvarsbegrensning var gjort gjeldende. Første faktura ble sendt 31. mars 2017. Tjenestene gjaldt ASP/brukertilgang og tilgang til Microsoft Office-pakke. Btec betalte kr 429,– pr ASP-bruker pr måned. Btec betalte kr 123,– pr Office-pakke-bruker pr måned. Det ble betalt kr 2760,– pr måned.

Btec fikk installert programmet Autocalc på Btecs server hos Nordlo. Autocalc er et prosjektbasert material- og produksjonssystem (MPS) for små og mellomstore produksjonsbedrifter i Norge. Det grunnleggende prinsippet i et MPS system er at produktene som bedriften skal produsere, beskrives i detalj basert på detaljerte produkttegninger. Programmet inneholder detaljerte anbud, kalkyler, tegninger, planleggingsdata,

produksjonsprogrammer, produksjonsmetodikk, informasjon om spesifikke komponenter og materialer, ordrehistorikk m.m. Nordlo var i dialog med leverandøren av programmet, Sigma 360, for å få installert programmet på serverne. Filene fra Autocalc ble lagret på RDS- serveren og ikke på filserveren. Nordlo tok en forhåndskopi fra Autocalc før innstallering og en ny kopi etter at Autocalc var installert og testet på Nordlos servere.

Den 21. april 2021 ble Nordlo utsatt for et alvorlig ransomware-angrep ved at trusselaktører logget seg inn på Nordlos nettverk via en såkalt «RD Gateway» som ledet til ax719rds, en terminalserveren tilhørende C. Påloggingen skjedde gjennom brukerkontoen til en av Nordlos kunder «post.hardmaler», som ikke krevde to faktorautorisering, fra Østerrike og Taiwan. Det er ikke kjent hvordan trusselaktørene fikk tak i kundens påloggingsdetaljer. Ved hjelp av denne tilgangen ble det sluppet et såkalt «cobalt strike beacon» på serveren. Aktiviteten via dette beaconet er ukjent, men mye trolig er det benyttet til å tilegne seg administrasjonsrettigheter. Det er imidlertid ikke kjent hvordan trusselaktørene fikk tilgang til admistratorrettighetene. Det fremgår av Ateas rapport at til tross for at servere ax719rds hadde godt patchenivå på operativssytemet, så hadde serveren gammel usupportert, upatchet og utdarter programvare som kan ha blitt utnyttet.

Trusselaktørene gikk fra RD-serveren og opp til domenekontroller, og slapp ytterligere to «beacons». Dette gjøres normalt for å lage flere veier til mål. Aktørene rekognoserte miljøet før de logget seg av kl. 0327. Nest dag kl. 1900 dag logget trusselaktørene seg inn igjen. De benyttet flere administratorkontoer for det IT-ekspertene kaller «lateral movement», og slo av antivirus innebygd i Microsoft og hentet ut angrepsdata. Trusselaktørene detonerte så «Ryuk ransomware» både manuelt og automatisk på en håndfull servere. En egenskap ved «Ryuk ransomware» er at den sprer seg selv til øvrige systemer ved eksekvering.

Hendelsen ble oppdaget av Nordlo sine systemer for overvåkning og varsling kort tid etter at angrepet ble iverksatt. Nordlo sitt personell stoppet angrepet og startet nedstengning av det rammede miljøet.

Etter angrepet iverksatte Nordlo strakstiltak, herunder passordbytte, manuell gjennomgang av servere og installasjon av EDR-løsning. De varslet sine kunder og samarbeidet med forsikringsselskap og eksterne sikkerhetsmiljøer.

Atea Incident Response Team ble av Nordlos forsikringsselskap, Tryg, engasjert for å kartlegge hendelsesforløpet, omfang og reetablere driften til Nordlo og tjenesten til kundene. Atea utarbeidet 01.06.2021 en rapport om hendelsesforløpet og håndtering av hendelsen.

Både Nordlo og deres kunder ble hardt rammet. I et par måneder etter cyberangrepet var det uvisst om man klarte å redde Btec sine data eller om disse var tapt. I midten av juni 2021 informerte imidlertid Nordlo AS om at dataene til Btec AS mest sannsynlig var tapt. Dette ble skriftlig bekreftet av daglig leder i Nordlo AS 02.12.2021. Videre ble det opplyst at av 255 kunder så var det bare 4 kunder som tapte alle data, hvorav Btec var en av disse 4.

For Btec sin del, medførte angrepet at det ikke var mulig å få tilbake data som Btec hadde lagret på RDS-serveren (ax1061rds), herunder informasjon som var lagret i Autocalc.

Data lagret på filserveren klarte en å gjenopprette da sikkerhetskopiene her var intakt.

Btec AS mistet som følge av angrepet all tilgang til sine data, inkludert ERP-system, produksjonsfiler, kundedokumentasjon og historiske kalkyler.

Btec måtte anskaffe nytt ERP-system (Sigma360), og bruke betydelige ressurser på å rekonstruere produksjonsdata, kundehistorikk og økonomisk dokumentasjon. Tapet førte til produksjonsstans, tap av kunder og økte kostnader, herunder revisjon og gjenoppbygging av systemer.

Btec anla ved stevning av 22.04.2024 fra advokat Solveig Charlotte Andersen søksmål ved Haugaland og Sunnhordland tingrett med krav om erstatning for det økonomiske tapet de var utsatt for etter at de mistet dataene sine etter dataangrepet mot Nordlo.

Nordlo tok rettidig til motmæle i tilsvar av 16.05.2024 fra advokat Tage Brigt Skoghøy og påsto seg frifunnet.

Hovedforhandling var opprinnelig berammet til 18.-20. november 2024.

Btec byttet prosessfullmektig til advokat Bodhild Kristine Høstmælingen.

Btec engasjerte sakkyndige til å vurdere om Nordlo kunne ha forhindret angrepet. De ble bedt om vurderinger av Nordlos sikkerhetstiltak, back-up løsning og gjenopprettingssystem på tidspunktet for ransomware-angrepet hos Nordlo i april 2021. Per Thorsheim avga rapport 01.11.2024. Defendable AS avga rapport 04.11.2024 og Deloitte AS avga rapport 04.11.2024.

Btec engasjerte også Defendable til å avgi en sakkyndig vurdering av de økonomiske konsekvensene. Denne rapporten ble fremlagt 04.11.2024 og kvalitetssikret av Deloitte AS.

Hensett til at disse rapportene kom kun kort tid forutfor hovedforhandlingen, ble saken begjært omberammet og Nordlo så seg også nødt til å innhent ny sakkyndighet til å vurdere Nordlos datasikkerhet.

Nordlo engasjerte EMP Secure for å gjennomgå sikkerheten i Nordlo. EMP Secure avgav rapport 12.05.2025.

Hovedforhandling ble avholdt 2. -6 juni 2025. Partene møtte med sine prosessfullmektiger samt rettslige medhjelpere. Det ble ført slik dokumentasjon og vitneførsel som fremgår av rettsboken. De sakkyndige vitnene var til stede under hovedforhandlingen og fikk anledning til å stille spørsmål til hverandre.

Saksøkerens påstandsgrunnlag

Btec AS gjør gjeldende at Nordlo Haugesund AS har begått et vesentlig kontraktsbrudd ved å ikke levere sikkerhetskopier som avtalt under den inngåtte ASP-avtalen.

Det forelå en muntlig avtale mellom partene, hvor Nordlo markedsførte sine tjenester som sikre og med daglig sikkerhetskopiering. Btec hadde derfor berettigede forventninger til at deres data ville være trygt lagret og tilgjengelig ved behov.

Etter avtalen påtok Nordlo seg helt konkrete forpliktelser med hensyn til sikkerhetskopiering og tilgjengelighet på data. Manglende sikkerhetskopiering og flere sikkerhetsbrudd representerer klare avvik fra det avtalte, og innebærer et brudd på grunnleggende krav til IKT-sikkerhet og avtalen om levering av ASP-tjenester. Nordlo har overfor Btec ikke presentert, og Btec ikke akseptert, noe lavere nivå på tjenestene, herunder sikker lagring og backup enn det som følger av faglig standard.

Nordlo påtok seg installasjon av nødvendig programvare slik som Autocalc, innrulling og lagring av data, herunder produksjonsdata hos Nordlo.

Heller ikke etterfølgende omstendigheter gir holdepunkter for at Nordlos plikter etter avtaleinngåelsen ikke handlet om sikkerhet og plikt til å sørge for backup.

Det foreligger et kontraktsbrudd da Nordlo hverken har levert sikker eller stabil leveranse. Nordlo har ikke levert backup i tråd med grunnleggende sikkerhet.

Btec anfører at det ikke er avtalt noen ansvarsbegrensning og det er ikke grunnlag for utfylling av avtalen. Tredjemann C kan verken pålegges byrder, forpliktelser eller begrensninger gjennom en kontrakt mellom A og B. Nordlo er klart nærmest til å ivareta de interessene som de har søkt å sikre seg gjennom avtalen med Deltapump AS også overfor andre. Den påberopte avtalen ble ikke presentert for Btec før lenge etter datatapet var et faktum, 28. mars 2022. Verken Btec eller A hadde noen tilknytning til Deltapump AS eller Nordlo fra før av.

Mot utfylling taler en betydelig overføring av risiko. Det har ikke vært omtalt mellom partene. I Agurkpinnedomen Rt-2004-675 var begrensninger vanlig i bransjen og betingelsene i det minste fulgte med. Enda mindre grunn til å godta det når det ikke er noe som er forelagt Btec og det ikke er ført bevis for hva som er vanlig.

Ansvarsfraskrivelsen gjelder kjernen i selve oppdraget til Nordlo: Backup og sikkerhet. Terskelen for vedtakelse må være høy, og terskelen for sensur gjennomgående være lav. Dette taler mot utfylling. Nordlo har risikoen for å unnlate gi opplysninger på en måte som gjorde Btec i stand til å se risikoen i Nordlos ytelse (og ukjente kontraktsvilkår). Btec ville ha tegnet forsikring om en fikk en klar oppfordring til det gjennom avtalevilkår. Grov uaktsomhet hos Nordlo taler også mot utfylling.

Subsidiært: Skulle retten mene at det er grunnlag for utfylling, må den anses bortfall pga grov skyld, lojalitetspliktsbrudd og grov uaktsomhet hos Nordlo.
Det er tale om gjennomgripende kontraktsbrudd med ingen tilgjengelig sikkerhetskopier.

Det er betydelig faglig svikt – det er i relasjon til kjerneytelsen mangelen oppstår – med svært stor skaderisiko. Det var ingen kontroll på backup, ingen skriftlige avtaler, ingen skriftlige rutiner. ASP-leveransens innhold representerte et markant avvik fra forsvarlig opptreden fra Nordlos side. En lang rekke brudd på NSMs grunnprinsipper. Manglende sikring er bekreftet av Defendable, Deloitte, Thorsheim, Atea og EMP. En lang rekke feil som i sum kvalifiserer til grov uaktsomhet. De kunne med rimelig enkle midler avverget hendelsesforløpet.

Nordlo har bevisbyrden for at det foreligger force majeure. Denne er ikke oppfylt. Angrepet mot Nordlo var påregnelig og ventet. Det var gjentatte varsler fra NSM. Trusselaktøren, Ryuk ransomware, som angrep Nordlo har vært aktiv siden 2018. Aktøren benyttet veletablerte og velkjente angrepsmetoder som sikkerhetsmyndigheter har advart mot i flere år før angrepet.

Btec anfører at Nordlo er ansvarlig for det tap som har oppstått, både på grunnlag av culpa og kontrollansvar. Det anføres også at Nordlo har handlet grovt uaktsomt.

NSMs grunnprinsipper for IKT-sikkerhet er bransjepraksis for IKT-virksomheter i Norge som selger denne typen tjeneste. De gjelder ikke bare for sikkerhetstjenester.

Nordlo har opptrådt uaktsomt ved ikke å sikre tilstrekkelig backup og ved å ikke iverksette nødvendige sikkerhetstiltak. Nordlo manglet flere helt grunnleggende sikkerhetstiltak som burde vært på plass hos enhver profesjonell leverandør av IT-tjenester.

Ateas rapport viser culpøs atferd, men den hadde et snevert mandat og undersøkte kun 1 av 1100 servere. Den skulle undersøke angrepsvektoren og gi anbefalinger knyttet til skadereduserende tiltak.

Det var svakheter i systemarkitektur og sikkerhetstiltak. Det ble bekreftet gjennom D at Nordlo ikke hadde skriftlige rutiner, segmentert backup for kundenettet eller sikkerhetsovervåkning. Nordlo oppdaget angrepet først når systemene var kryptert. Det er bekreftet at administratorkontoer ikke hadde flerfaktorautentisering på bruk på interne servere. Det er ikke fremlagt informasjon som tilsier at systemet var konfigurert for sikkerhetsovervåkning. Det fremstår som om det var bare for drift.

Det er ikke fremlagt informasjon som tilsier at syslog var konfigurert for sikkerhetsovervåkning.

Sikkerhetskopiering og segmentering var mangelfull. Nordlo unnlot å presisere at disse sikkerhetstiltakene ikke gjaldt for kundenettet. Backup i kundenettet var ikke segmentert og lå i samme nettverk som kundedata for øvrig (Prodnett1). Nordlo har ikke gitt Btec informasjon om risikoen Btec løp ved å la Nordlo «forvalte» dataene sine slik Nordlo gjorde. Valget er svært uheldig, når skadepotensialet er stort. Konsekvensene av Nordlos valg er heller aldri forelagt Btec. Det er brudd på alminnelig lojalitetsplikt.

Det var grunnleggende mangel på rutiner i sin alminnelighet. Nordlo hadde ingen styringssystem for informasjonssikkerhet, herunder rutiner, prosesser eller prosedyrer for sikkerhet. Det er et klart avvik fra hva man bør forvente av den profesjonell IT-leverandør.

Nordlo har ikke implementert grunnleggende sikkerhetstiltak for å unngå angrepet. Dette er bekreftet av rapportene og forklaringene til Defendable, Deloitte og Thorsheim.

Manglende er som følger: Generelt svært svak etterlevelse av NSMs grunnprinsipper for sikkerhet, Ingen moderne endepunktsikring (EDR/EDR) og svak kontroll over endepunkter, Unødvendig bruk av for høye rettigheter og svært svak tilgangskontroll, svært svak kontroll over nettverkstrafikk, Nordlo hadde svak kontroll rundt oppdatering av programvare. Nordlo sine eksponerte tjenester (DRP) benyttet ikke oppdatert programvare med de siste sikkerhetsfikser. Atea og Torsheim peker på dette en av de to mest aktuelle inngrepsvektorene for angrepet. Videre var det mangelfull logging og overvåkning av kritiske systemer. Nordlo benytter seg kun av SNMP – et enkelt driftsovervåkningsverktøy som overhodet ikke er egnet som sikkerhetsovervåkningsverktøy. Det var videre manglende segmentering og skille mellom operativt nettverk og kunders nettverk, samt mellom kunder, brudd på NSM grunnprinsipp 2.5 og 2.2.3, 2.2.4 og 2.2.5.

Nordlo lagret filer på «terminalserveren». Det kunne og burde vært annerledes. Det var Nordlo som satte opp tjenesten. Nordlo visste beviselig at det var store mengder produksjonsdata knyttet til denne.

Det var ikke implementert grunnleggende sikkerhetstiltak for å sikre backup. Det ble bekreftet i Ds forklaring at backup-server i prodnett1 (det risikofylte kundenettet) var ikke skilt ut. De har ikke fulgt 3-2-1 regelen og kan ikke ha testet backup eller hatt rutinger. At Nordlo velger å ikke følge grunnleggende prinsipper for sikkerhetskopiering er klart uaktsomt. Nordlo har aktivt og bevisst unnlatt å implementere sikkerhetstiltak rettet

mot prodnett1, selv etter at det ble ansett nødvendig med økt sikkerhet i 2019. At det finnes flere selskaper som har like dårlig sikkerhet som Nordlo er ikke en unnskyldning eller en korrekt representasjon av normalen i bransjen.

Profesjonelle IT-leverandører som Nordlo forventes å følge anerkjente sikkerhetsstandarder, ikke å senke seg til laveste nivå.

De samme hensyn gjør seg gjeldende både i forhold til culpaansvaret, kontrollansvaret og vurderingen av om det er opptrådt grovt uaktsomt.

Det er ikke tvilsomt at det er årsakssammenheng mellom Nordlos handlinger og unnlatelser og Btecs påførte skade og tap. Det er ikke bare et enkelt tiltak. Her er det massivt. Hadde en enkelt faktor vært på plass ville vi ikke ha stått her i dag. 14 faser i angrepskjeden. Det var full kollaps hos Nordlo. De evnet kun å avdekke krypteringen. Hadde Nordlo tatt backup,som de skulle, ville skaden ikke ha skjedd De tok ikke backup og sørget ikke for at den var lagret forsvarlig vis. Tvilsrisikoen må uansett plasseres hos skadevolderen dersom årsaksforholdet er uklart, jf. Nygaard LoR 2000.

Btec har sannsynliggjort et økonomisk tap i størrelsesorden 55-62 millioner kroner. Dersom en tenker datatapet tenkt borte, ville Btec ha fulgt markedsutviklingen, ikke måttet selge maskinparken, ikke tapt varelager, ikke økt revisorkostnader, ikke tapt oppdrag, ikke tapt fortjeneste, ikke måttet bygge opp nytt ERP-system. Grunnlaget for kravet bygger på grundige vurderingen fra Defendable som basere seg på kombinert regnskapsanalyse, årsregnskap, tilgjengelig regnskap fra samarbeidspartnere og bedrifter. Det var grundig og analytisk gjennomgåelse og Deloitte vurdert metodikk. De har gått over årsregnskaper med noter fra Btec. Analyser av regnskapet til kunder, samarbeidspartnere og konkurrenter, sjekket mot eksisterende tall i virksomheten, undersøkt fakturaer, oppstillinger og beregninger. De har tilnærmet seg konkurrenter metodisk og kontrollert sammenligningsgrunnlagene, intervjuet kunder, samarbeidspartnere og konkurrenter og mottatt tallmateriale fra enkelte kunder som viser historikk hva angår bestillinger fra Btec før/etter angrepet i april 2021. Det er ikke tvilsomt at Btec ble påført betydelige økonomiske tap.

De fikk umiddelbare likviditetsutfordringer, produksjonsutfordringer, påvirkning på eksisterende leveranser, påvirkning på nye leveranser/bestillinger, påvirkning på verdi av varelager, påvirkning på ERP-systemet, påvirkning på regnskapsavleggelse. De ble rammet på et tidspunkt hvor veksten i bransjen var bra, men uten at de fikk samme mulighet til å utnytte dette som dersom datatapet ikke hadde skjedd.

Det er sannsynliggjort et økonomisk tap for tap av modeller og kalkyler. Det er sannsynliggjort at 70-80 % av ordrene er basert på historisk data. Defendable har brukt en kostnadsbasert tilnærming om hvilke merkostnader har Btec hatt som følge av tapet. Dette er en anerkjent metode. Det er videre sannsynliggjort et omsetningstap der en har brukt en inntjeningsbasert metode med forskjellene i inntjening sammenholdt med dersom Btec hadde fått dataene tilbake fra Nordlo. Det er videre sannsynliggjort tap ved salg av 11 maskiner i maskinparken. Det er innhentet priser på gjenanskaffelse. Det er en kostnadsbasert anerkjent metode. Det er videre sannsynliggjort merkostnader til å implementere ERP- system. Også her er det benyttet en kostnadsbasert tilnærming og anerkjent metode. Systemet må gjenopprettes og det tar tid.

Btec har også lidd et økonomisk tap ved at en ikke kan selge deler på varelageret som ikke er sporbare. Dette er et krav i bransjen.

Revisor har også brukt betydelig mer tid på revisjon og kravet bygger på en uttalelse fra revisor.

Et eventuelt erstatningsbeløp være skattepliktig for Btec og det er derfor ikke trukket i fra skatt fra tapspostene

Btec mener det ikke foreligger grunnlag for lemping av erstatningsansvaret. Det er her et stort men ikke upåregnelig tap. Det er alminnelig kjent i bransjen at store tap utløses ved mangelfull beskyttelse mot cyberangrep. De har likevel forholdt seg svært avslappet til grunnleggende sikkerhet og alminnelige beskyttelsestiltak. Det er ikke anført at de ikke har økonomisk bæreevne. Nordlo burde hatt forsikringer som kunne dekket slike hendelser. Avtalen inngått på en måte som Nordlo hadde full kontroll på. Det er ikke rimelig at Btec skal bære risikoen for Nordlos forhold.

Videre krever Btec full dekning for sakskostnader, inkludert utgifter til sakkyndige. Sakens kompleksitet tilsa behov for sakkyndighet og manglende bevistilgang har vært fordyrende.

Saksøkerens påstand

1. Nordlo Haugesund AS betaler erstatning til Btec AS etter rettens skjønn

2. Btec AS tilkjenner sakskostnader.

Saksøktes påstandsgrunnlag

Nordlo bestrider at det foreligger grunnlag for erstatningsansvar overfor Btec som følge av det omtvistede cyberangrepet og det påståtte datatapet.

Nordlo har oppfylt sine forpliktelser som leverandør av ASP-tjenester til Btec, og bestrider erstatningskravet fremsatt.

For det første anfører Nordlo at det foreligger en gyldig og bindende avtale mellom partene, og at denne avtalen bygger på selskapets standardvilkår for levering av ASP-tjenester. Det vises til at Btec trådte inn i et eksisterende avtaleforhold som tidligere var inngått med Delta Maskinering, og at det aldri ble presentert andre vilkår enn de som fulgte av denne avtalen. Nordlo gjør gjeldende at Btec var kjent med, eller i det minste burde ha vært kjent med, disse vilkårene, og at det derfor ikke er grunnlag for å hevde at avtalen er vilkårsløs eller mangelfullt regulert. Btec har vedtatt Nordlos standardvilkår for levering av ASP-tjenester. A overtok som daglig leder i Delta Maskinering, og fikk en innføring i ASP-leveransen av E i Delta Maskinering. A ga Nordlo beskjed om å opprette ASP-brukere også for Btec og uttalte at han ville samkjøre bedriftene. Btec ønsket ikke å delta på oppstartsmøte.

Avtalen må uansett utfylles av bransjevilkårene. Vilkårene er vanlige i bransjen, jf. IKT Norges standardvilkår og Statens standardavtale for IT-anskaffelser. Risikofordelingen mellom leverandøren og kunden må ses i lys av de begrensede månedlige vederlagene. Det var en felles forutsetning mellom partene at tjenesten skulle reguleres av samme vilkår som Delta Maskinering.

Nordlo anfører videre at selskapet har levert de avtalte tjenestene i samsvar med kontrakten, herunder drift og tilgjengeliggjøring av dataprogrammer, samt sikkerhetskopiering av kundens data.

Avtalen gjelder drift og tilgjengeliggjøring av dataprogrammer via internett (servere i datasentral og påloggingsløsning via nett), inkludert en oppetids- og responsgaranti. Leverandøren skal ta og lagre sikkerhetskopier av kundens data. Det er en tydelig risikofordeling mellom partene. Leverandøren påtar seg ikke kundens forretningsrisiko. Nordlo tilbyr ikke forsikringstjenester. Tjenesten må ses i lys av det månedlige vederlaget. Btec har ikke betalt for å lempe forretningsrisikoen over på Nordlo. I pkt. 8 i avtalen er det avtalt at ved hindringer utenfor partens kontroll suspenderes partenes plikter. Utenfor kontroll er ikke bare begrenset til force majeure. I pkt. 10 er det avtalt ansvarsbegrensninger om at kunden ikke kan kreve erstatning for indirekte tap og at kundens erstatningskrav kan ikke overstige tre månedsleier.

Nordlo har driftet og tilgjengeliggjort programmene overfor Btec i henhold til avtalen, foruten om nedetidsperioden i april – mai 2021. Nordlo har vitterlig hatt fokus på sikkerhet Det ble benyttet to datasenter hvor kundeservere og kritisk infrastruktur var delt mellom disse. Datasentrene hadde gode løsninger innen strøm, kjøling og nettverk. Det ble tatt daglig backup fra begge datasenter. Backup ble tatt til «motsatt datasenter» for å skille backup fysisk fra produksjon. Nordlo hadde segmentert ut det meste av kritisk infrastruktur inkludert backup i eget nett. Dette nettet (backbone, managementnett, administrasjonsplan) hadde eget domene og følgelig også egne brukerkontoer. Managementnettet ble aldri rammet av angrepet og segmenteringen fungerte altså etter hensikten. Nordlo hadde segmentert kunder i 3 ulike prodnett. (Flest kunder på prodnett1 som ble rammet) Nordlo benyttet MFA på alle kontoer i management nettet. Det var installert antivirus på alle servere. Det var implementert brannmur som et sikkerhetslag. De hadde gode rutiner for oppdatering av operativsystem på serverne

Det forelå ingen indikasjon på lagring av virksomhetskritiske data i ASP-løsningen. Det har blitt tatt sikkerhetskopier i tråd med avtalen. Det har blitt gjennomført sikkerhetskopiering av begge Btecs servere, RDS-serveren (ax1061rds) og filserveren (ax1062file)

Dataene som var tatt backup av fra filserveren ble gjenopprettet etter angrepet, og tilbakelevert til Btec. Nordlo ble ikke orientert om lagring av virksomhetskritiske data gjennom Autocalc.

Cyberangrep lykkes overfor de «beste», og er ikke i seg selv et tegn på manglende kvalitet Et enkelt tiltak ville kanskje kunne forsinket angrepet, men det er ikke slik at et enkelt tiltak alene kunne forhindret angrepet. Krypteringen skyldtes hackernes profesjonalitet.

Cyberangrepet var utenfor Nordlos kontroll, jf. avtalen punkt 8. Btec har ikke forsikret verdien av egne data, slik de plikter etter avtalen, og må selv bære risikoen for dette.

Det bestrides at det foreligger noe ansvarsgrunnlag hverken i forhold til kontrollansvar, culpa eller grovt uaktsomhet.

Nordlo har ikke opptrådt erstatningsbetingende uaktsomt. Hvilke sikkerhetstiltak og -systemer som kan forventes, må ses i lys av hva Btec som ASP-kunde har kjøpt og betalt for.Det er alltid mulig å implementere ytterligere sikkerhetstiltak, men ikke gitt at det vil ha særlig effekt. Btec har verken stilt krav eller kjøpt IT-sikkerhet/ rådgivning

Når det gjelder selve cyberangrepet, gjør Nordlo gjeldende at dette var et avansert og målrettet angrep utført av profesjonelle trusselaktører, og at angrepet lå utenfor selskapets kontroll. Nordlo har implementert nødvendige sikkerhetstiltak og -systemer for å gardere seg best mulig mot eventuelle cyberangrep. Nordlo anfører at det ikke er grunnlag for å hevde at selskapet har opptrådt uaktsomt, og at det ikke foreligger noe erstatningsbetingende forhold. Det ble tatt daglige backup av kundenes data, og månedlige backup for langtidslagring Det var daglige rutiner for sjekk av brannmurer, backup, mv, automatisk overvåkning og varsling ved spesielle hendelser eller problemer med tjenestene (SNMP-basert overvåkningssystem, ukentlig sårbarhetsscanning av systemene for å oppdage eventuelle utdaterte programmer og sårbare konfigurasjoner (MPS). Kritisk infrastruktur og backup av filserver var segmentert ut i eget nett (management-nettet). Kunder var segmentert i tre ulike prodnett. Nordlo visste ingenting om Btec og hva som var virksomhetskritisk Kundene fikk tilbud om MFA-sikring (flerfaktorautentisering) på tjenestene som støtte det, men måtte selv velge tjenesten. Btec hadde ingen forventning om MFA-sikring; de kjente tvert om til at det ikke var påkrevd. Det var flerfaktorautentisering på administrative kontoer. Det ble benyttet sentral logging til syslog fra forskjellige systemer. Nordlo har ikke opptrådt erstatningsbetingende uaktsomt ved å ikke greie å forhindre cyberangrepet.

I forhold til økonomisk tap og årsakssammenheng anføres det prinsipalt at et eventuelt erstatningsansvar er undergitt ansvarsbegrensninger etter avtalens pkt. 10 eller bransjevilkår. Btec kan ikke kreve erstatning for indirekte tap. Erstatningsansvaret kan ikke overstige tre, evt. maksimalt 12, ganger det månedlige vederlaget

Subsidiært anføres det at de anførte tapspostene er udokumenterte. Atter subsidiært anføres det at de anførte tapspostene står ikke i adekvat årsakssammenheng med misligholdet.

Nordlo bestrider at det foreligger tilstrekkelig dokumentasjon for de påståtte økonomiske tapene. Det gjøres gjeldende at Btec ikke har sannsynliggjort at det foreligger et økonomisk tap som står i adekvat årsakssammenheng med det påståtte kontraktsbruddet.

De ulike tapspostene, herunder tap av kalkyler og modeller, omsetningstap, salgstap ved avhending av maskiner, kostnader til nytt ERP-system, tap av varelagerets verdi og økte revisjonskostnader, er etter Nordlos syn ikke tilstrekkelig dokumentert. Det vises til at beregningene bygger på antakelser og generelle vurderinger, og at det mangler tidsnære og etterprøvbare bevis.

Ved kravet om erstatning for tap av kalkyler og modeller er det ikke ført bevis for at 70 % av produksjonen var basert på historiske data, ei heller gjennomsnittlig produksjonstid på 6 timer. Det anførte tapet på kr 21,8 millioner er ikke dokumentert.

For å kunne kreve erstatning for omsetningstap, må Btec dokumentere at avtaler har falt bort eller ikke blitt inngått som følge av datatapet. Det er ikke fremlagt tidsnære bevis. F uttalte i sin vitneforklaring at Servogear AS hadde til hensikt å nedskalere sine bestillinger hos Btec fra 2020. Defendable har beregnet seg frem til at bransjen sammenlignet med 2020 har hatt en gjennomsnittlig omsetningsvekst på henholdsvis 1,4 % for 2021, 37,2 % for 2022 og 76,7 % for 2023. Servogear hadde allerede før angrepet besluttet å sette ut arbeid til flere enn Btec; gikk fra 4 til 10 leverandører. Btec har selv endret maskinparken sin, slik at den ikke er like kompatibel med Servogears bestillinger lenger. G forklarte at det var turbulente år fra og med 2020. Fra slutten av 2021 tok markedet seg opp.

Btec hevder de fikk likviditetsutfordringer som følge av datatapet, og ble tvunget til å selge CNC-maskiner med salgstap på kr 10-14,7 mill. Det er verken fremlagt dokumentasjon for likviditetsutfordringene, nødvendigheten av salgene eller sammenhengen med datatapet.

Nordlo bestrider at det er grunnlag for å kreve erstatning på kr 1,9 – 3,7 millioner for bytte av ERP-system. Det er ikke fremlagt noen dokumentasjon for å underbygge antall konsulenter, måneder eller timepris.

Nordlo kan ikke holdes erstatningsansvarlig basert på generelle uttalelser om at varelageret har tapt seg i verdi.

Det er ikke ført bevis for tap av data har ført til 1,2 millioner i økte revisjonskostnader.

Nordlo gjør også gjeldende at det uansett foreligger avtalte ansvarsbegrensninger som begrenser et eventuelt erstatningsansvar til tre måneders vederlag. Det vises til at slike begrensninger er vanlige i bransjen, og at det ikke er grunnlag for å fravike disse. I tillegg anfører selskapet at de påståtte tapene i stor grad må anses som indirekte tap, som etter avtalen ikke kan kreves erstattet.

Endelig gjør Nordlo gjeldende at et eventuelt erstatningsansvar må lempes. Det vises til at det påståtte tapet er ekstraordinært stort sammenlignet med det månedlige vederlaget for tjenestene. Btec er selv skyld i at cyberangrepet fikk de konsekvensene det fikk for deres virksomhet. Btec stilte ikke på oppstartsmøte. Nordlo ble heller ikke informert om innholdet eller verdien av dataene som ble lagt inn. Nordlo ble ikke informert om hva som var virksomhetskritisk for Btec. Nordlo hadde ikke noen foranledning til å iverksette ytterligere tiltak for å sikre Autocalc-dataene. Det fremheves at Btec selv stod nærmest til å forsikre verdien av egne data, og at selskapet ikke har tatt nødvendige forholdsregler for å beskytte seg mot konsekvensene av et eventuelt datatap. Nordlo anfører at det ikke er vanlig for ASP-leverandører å påta seg ansvar for kundens forretningsrisiko, og at det heller ikke er vanlig å tegne forsikringer som dekker slike tap.

Nordlo er ikke å bebreide for cyberangrepet og konsekvensene det fikk. Cyberangrepet ble gjennomført av profesjonelle trusselaktører. Angrepet var avansert og systematisk gjennomført. Nordlo hadde iverksatt en rekke sikkerhetstiltak og -rutiner, noe som gjorde at angrepets omfang ble begrenset vesentlig Det er ikke slik at et konkret sikkerhetstiltak ville forhindret cyberangrepet. Det ble tatt sikkerhetskopier av alle kjente kritiske data.

Erstatningsansvaret vil virke urimelig tyngende, og må lempes

Saksøktes påstand

1. Nordlo Haugesund AS frifinnes.
2. Btec AS dømmes til å erstatte sakskostnadene.

Rettens vurdering

Retten skal ta stilling til om Nordlo har oppfylt sine forpliktelser etter avtalen. Retten må da først ta stilling til om Btec har vedtatt Nordlos standardvilkår og eventuelt om avtalen må utfylles med bransjevilkår.

Retten skal videre ta stilling til om Nordlo har opptrådt i strid med bransjestandarder, om det foreligger ansvarsgrunnlag og årsakssammenheng, og om Btec har dokumentert sitt økonomiske tap i tilstrekkelig grad. Saken reiser spørsmål om IT-leverandørers ansvar ved cyberangrep og betydningen av sikkerhetsrutiner og avtalevilkår i ASP-leveranser.

ASP er forkortelsen for «Application Service Provider» og innebærer at Nordlo var leverandør av IT-tjenester over internett, altså en sentralisert driftstjeneste hvor Nordlo driftet en datasentral som forvaltet/ tilgjengeliggjorde kundenes data og applikasjoner med en påloggingsløsning via nett.

ASP-tjenester kan være svært gunstige for små og mellomstore bedrifter som ønsker en kostnadseffektiv og sikker IT-løsning uten å bygge opp egen IT-avdeling. Fordelen med ASP- tjenester er at en betaler en fast månedssum til en it- leverandør og slipper investering i egne servere, programvare og driftspersonell. Hele prinsippet for ASP er at flere kunder deler fysisk infrastruktur som servere, brannmurer, backupløsninger etc. for å oppnå en kostnadseffektiv it-leveranse. Dette medfører også en sikkerhetsrisiko ved at en deler infrastruktur med andre kunder.

***

Avtalen:

Retten tar først stilling til hva som er avtalt mellom partene. Partene er enig om at det mellom Btec og Nordlo i mars 2017 inngått en avtale om ASP-løsning, hvor Btec fikk tilgang til sine applikasjoner og data via Nordlos

servere. Det foreligger imidlertid ingen signert kontrakt mellom partene der vilkårene for avtalen eksplisitt fremgår.

Spørsmålet er om Btec må anses bundet av Nordlos standardkontrakt og vilkårene om ansvarsfraskrivelse i pkt. 8 og 10 således kan gjøres gjeldende.

Avtalefriheten bygger på et ideal om at to jevnbyrdige parter inngår avtaler etter sin frie vilje. I vår tid inngås mange avtaler etter standarddokumenter – kontraktsmaler – som er utarbeidet av leverandører av varer og tjenester. Kontraktsmalene er utarbeidet med sikte på fremtidige avtaleinngåelser, og skal kunne tilsluttes av forbrukere eller næringsdrivende, uten at disse har påvirket innholdet.

Det har ikke vært noen bevisførsel som viser at bestemmelsene om ansvarsbegrensninger har vært omtalt i forhandlingene mellom partene. Selve inngåelsen av avtalen baserer seg i all hovedsak på muntlige samtaler mellom partene som resulterte i at Nordlo opprettet brukere til Btec og det ble betalt en månedlig sum pr bruker.

Den skriftlige avtalen mellom Delta Pump og Nordlo av 11.02.20211 må anses for å være en avtale mellom andre rettssubjekter enn partene i herværende sak. I denne avtalen fremgår ansvarsbegrensningene uttrykkelig.

Det eneste tidsnære beviset som foreligger i saken er en logg av 01.03.2017 som viser at hovedaksjonær og daglig leder i Btec, As, tok kontakt på telefon med Nordlo og ba om at det ble opprettet ASP. Det fremgår av loggen at *A har kjøpt opp delta maskinering og har et firma på Bømlo med 15 ansatte. Han ønsker å kunne samkjøre disse bedriftene. Med ASP, men ville ha et teknisk møte for å avgjøre hvordan dette kunne løses.... Har avtalt møte 2 ganger uten at han har dukket opp, svarer heller ikke på mail. Ballen ligger hos han nå.*

Btec ble innkalt til to møter med Appex, men møtte ikke til disse og ASP-løsningen ble tatt i bruk uten at det ble signert noen skriftlig kontrakt.

Btec betalt kr. 429,– pr ASP-bruker pr måned og kr. 123,– pr Office-pakke-bruker pr måned. Totalt ble det betalt kr. 2760,– pr måned fra november 2017.

Retten finner at det er en svakhet at Nordlo ikke har sørget for å få en signert skriftlig avtale før ASP- tjenesten ble levert Det vil være Nordlo som har bevisbyrden for at standardavtalen med ansvarsfraskrivelsene kan gjøres gjeldende.

Høyesterett har åpnet for at kunder som har sluttet seg til standardavtaler kan være ubundet av et vilkår, mens andre deler av standardavtalen gjelder. Problemet blir ofte stilt som om vilkåret er vedtatt.

Det fremgår av Giertsen Avtaler av 2021s 92:

> *Problemet kan formuleres som ellers ved avtalebinding – om vare- eller tjenesteyteren kan ha en berettiget forventning om at kunden har vedtatt vilkåret. Hvis kunden kjente til standardvilkårene ved avtaleinngåelsen og forstod hva disse innebar, er vilkårene normalt vedtatt. Det er som regel tale om en underforstått vedtakelse, ved å bestille varen eller tjenesten med kunnskap om leverandørens avtalevilkår.....*
>
> *Problemet er så hvordan vedtakelsesspørsmålet stiller seg hvis avtalen inngås ved en handling – kjøre inn på en ferge, stige på bussen mv. – og kunden ikke kjenner vilkårene. Slik uvitenhet kan av minst to grunner ikke utelukke underforstått vedtakelse. For det første vil kunden som regel forstå at vare- eller tjenesteyteren må ha vilkår for sin yteplikt; som pris, betalingstidspunkt etc. For det andre tilsier effektiviteten i det økonomiske livet at det må være rom for binding til standardvilkår, særlig der samme type avtale inngås hyppig som transport, strøm, telefon, forsikring osv. Hvis kundene bare bindes til standardvilkår ved uttrykkelig vedtakelse, vil kostnadene med slike transaksjoner stige, til ulempe for kundene. Leverandøren av varen eller tjenesten må på den andre siden søke å informere kundene om vilkårene (nettsider, oppslag i forretninger mv.). Om et standardvilkår er vedtatt, vil bero på en avveining av disse hensynene.*
>
> *Hvis en standardavtale har vært brukt i en viss tid, og aktørene i bransjen har innrettet seg i lys av denne, kan det i seg selv være et tegn på kvalitet – i den forstand at aktørene legger til grunn at den er balansert. Brukes en slik standardavtale, kan det gi en særlig grunn til å anta at kundene (underforstått) har vedtatt vilkårene. Utbredelsen var i kortslutningsdommen et argument for å legge vilkåret til grunn. Høyesterett gikk «ut fra at en fraskrivelse av ansvar på objektivt grunnlag, som ... i*

dette tilfelle, er vanlig i strømleiekontrakter ved de forskjellige kra.verker» (Rt-1964-838 på s. 841). En ansvarsfraskrivelse i e-verkets standardvilkår var vedtatt.

Det kan oppstå spørsmål om hyppig brukte standardvilkår kan danne grunnlag for en bransjepraksis som blir en (tung) kilde når det gjelder innholdet av bakgrunnsretten. Det er da sentralt om vilkåret er brukt i lang tid, om det er utbredt i bransjen, om aktørene i bransjen har fulgt det fordi det anses bindende, og om det er balansert.

Rt-1973-967 spedisjonsdommen: Høyesterett viste til «at *når det ... foreligger innarbeidede bransjeregler [på bakgrunn av Nordisk Speditørforbunds standardkontrakt], og disse verken kan anses uvanlige eller urimelige ... må kontrakten i mangel av annen avtale anses inngått på bransjens vanlige vilkår*» (s. 971). I denne dommen hadde standardvilkårene vært så utbredt i femti år at Høyesterett la til grunn at avtalens vilkår regulerte kontraktsforholdet på det aktuelle punktet, selv om partene ikke hadde vist til standardkontrakten.

I Rt-1964-838 ved bestilling av strøm ble det lagt til grunn at selv om kunden hadde bestilt muntlig på telefon ble han likevel bundet av standardvilkårene. Det var ikke et krav om at kunden hadde satt seg inn i vilkårene. Det ble lagt vekt på at kunden måtte vite at det forelå bestemmelser om forholdet og vilkårene var vanlige i bransjen.

Retten finner det sannsynliggjort at Btec var, eller burde vært kjent med Nordlos standardvilkår for levering av ASP- tjenester.

Delta Pump ved Carl Johan B inngikk skriftlig avtale om levering av ASP-tjenester 11.02.2011. Litt senere ble Delta Maskinering, et datterselskap av Delta Pump, innlemmet i avtaleforholdet. Det foreligger heller ikke her noen skriftlig avtale, men hensett til at det var samme eiere og samme ledelse i begge selskapene usannsynlig at det her ble fremforhandlet andre vilkår og retten legger det til grunn som sannsynliggjort at de samme vilkårene ble gjort gjeldende i forhold til Delta Maskinering som i Delta Pump.

Btec overtok Delta Maskinering vederlagsfritt i februar 2017. A overtok som daglig leder i Delta Maskinering og fortalte under sin partsforklaring at han fikk en innføring i ASP- leveransen av en E i Delta Maskinering. Han fikk en egen bruker i Delta Maskinering. I Btec hadde de servere til noen hundretusen. De vurderte at de var mer tjent med å gå over til en ASP-løsning også i Btec. Det fremgår av det eneste tidsnære beviset at A opplyste at han ønsket å samkjøre disse to bedriftene. Dette tyder på at A var kjent med avtalen og løsningen som Delta Maskinering hadde.

Det er ikke fremlagt noen som helst beviser på at Btec fremforhandlet seg andre vilkår enn det som fremgikk av standardavtalen til Nordlo som de brukte på sine kunder. Btec ble innkalt til to oppstartsmøter, men møtte ikke til noen av dem.

Første faktura med fakturering for etablering av servere og Appex ASP ble sendt 31.03.2017, altså kort tid etter at telefonsamtalen med Nordlo fant sted.

Det ble betalt kr 429,– pr ASP bruker pr måned. Når en hensyntar den generelle prisstigningen siden 2011 til 2017, samsvarer det månedlige beløpet med summen som ble betalt for Delta Pump.

Når A bestiller samme tjenesten til Btec som Delta Maskinering og bevisst unnlater å møte til møter hvor gjennomgang av vilkårene var en naturlig del, finner retten at Btec er den nærmeste til å bære risikoen for dette. Når Btec tar i bruk tjenesten og betaler det månedlige beløpet for tjenesten som følger av Nordlos alminnelige vilkår, i finner retten at det her må anses for å foreligge en underforstått vedtakelse av de alminnelige vilkårene til Nordlo.

Retten har også lagt vekt på at vilkårene er vanlige i bransjen. Både IKT Norges Standardvilkår og Statens standardavtale for IT- anskaffelser har tilsvarende ansvarsbegrensninger og avgrenser mot indirekte tapsposter.

Både sakkyndig vitne Olav Espedal fra it-firmaet EMP- Secure og Per Øyvind Arvid Thorsheim fra it- firmaet Tietoevery bekreftet at slike avtaler er vanlig i bransjen.

Retten finner at det har formodningen mot seg at det ble inngått en vilkårsløs avtale.

Retten finner at det var en felles forutsetning mellom partene at tjenesten skulle reguleres av samme vilkår som Delta Maskinering.

Risikofordelingen mellom leverandøren og kunden må også ses i lys av de begrensede månedlige vederlagene. Btecs månedlige betaling for tjenesten var kr. 2760,– fra november 2017. Et slikt månedlig vederlag samsvarer

ikke med at Nordlo skal ha påtatt seg en forretningsrisiko på over kr. 60 millioner. Retten finner at det har formodningen mot seg at Nordlo skulle påta seg et slikt ansvar til et slikt beskjedent beløp.

Det fremgår av standardavtalens punkt 3 at kunden er selv ansvarlig for å forsikre verdien av egne data.

A forklarte selv under sin partsforklaring at de hadde helseforsikringer, forsikring på maskinene og avbruddsforsikring og at de totalt betalte kr. 60 000,– i måneden i forsikringer. Retten finner at det da har formodningen mot seg at Btec skulle ha en berettiget forventning om at de vilkårsløst skulle inngå en avtale som skulle medføre at Btec skulle ha påtatt seg en forretningsrisiko på over kr 60 millioner.

Andre aktører i bransjen, blant annet G production, bekreftet i retten at de hadde egne avbruddsforsikringer og cyberforsikringer. Dette taler også mot at Btec skulle ha en forventning om at de inngikk et ASP-avtale uten noen som helst begrensninger hva gjelder økonomisk ansvar.

Uten ansvarsbegrensningene som fulgte av Nordlos standardavtale, som var i tråd med bransjepraksis, ville ASP leverandøren fungert som et rent forsikringsselskap.

Retten finner etter dette at Btec må anses for å være bundet av Nordlos standardavtale med de gjeldende begrensninger som der fremgår, selv om de ikke uttrykkelig har vedtatt disse.

****

Force Majeure:

Det fremgår av avtalens pkt. 1 at leverandøren påtar seg ansvaret for drift av kundens dataprogrammer og skal gjøre disse tilgjengelige via Internett. Kunden har tilgang til support i arbeidstiden i virkedager og ut over dette blir det etablert en bakvaktstelefon. Appex garanterer 99,5 % oppetid. Det fremgår av avtalen at Appex tar sikkerhetskopier av kundens data hver virkedag. Dersom kunden ber om det, skal leverandøren tilbakekopiere angitte data fra siste sikkerhetskopi.

Det følger av punkt 10 i avtalene at «*Det foreligger mangelfulle tjenester dersom tjenestene etter Oppstartsdag ikke oppfyller de krav som fremgår av denne Avtalen.»*

Nordlo har gjort gjeldende at det forelå en «force majeure» hendelse – i det angrepet var «utenfor Nordlos kontroll», hvor det da følger av avtalene at partenes plikter overfor hverandre suspenderes i den perioden tilstanden vedvarer.

I pkt. 8 i avtalen fremgår det følgende:

> *Dersom Avtalens gjennomføring helt eller delvis hindres, eller i vesentlig grad vanskeliggjøres av forhold som ligger utenfor partenes kontroll, suspenderes partenes plikter i den utstrekning forholdet er relevant, og for så lang tid som forholdet varer. Slike forhold inkluderer, men er ikke begrenset til, streik, lockout, og ethvert forhold som etter norsk rett kan bli bedømt som force majeure.*

Nordlo har anført at de har driftet og tilgjengeliggjort programmene overfor Btec ihht. til avtalen, foruten nedetidsperioden april- mai 2021. De har hatt fokus på sikkerhet og tatt sikkerhetskopier i tråd med avtalen. Dataangrepet var utenfor Nordlos kontroll etter avtalens pkt. 8.

Om vurderingen av «kontrollsfæren» har Høyesterett i Rt-2022-192-A [skal vel være HR-2022-192-A, Lovdatas anm.], avsnitt 72, uttalt følgende:

> «*Oppsummeringsvis legger jeg etter dette til grunn at vilkåret om at årsaken til mangelen må ligge utenfor selskapets kontroll, må vurderes konkret. Det avgjørende er om årsaken ligger innenfor det selgeren – etter en objektiv vurdering – kunne kontrollere eller påvirke gjennom planlegging, styring og kontroll med virksomheten. Foreligger det handlingsalternativer for selger som ville ha forhindret årsaken til mangelen, ligger årsaken normalt innenfor selgers kontroll, med mindre årsaken skyldes ekstraordinære forhold. Det er ikke avgjørende om selgeren har opptrådt aktsomt.»*

Retten viser også til Rt-2008-537, avsnitt 58, hvor det fremgår det at:

> «*Innenfor kontrakts-retten er den alminnelige regel antatt å være at debitor ved mislighold av generisk bestemte forpliktelser hefter på objektivt grunnlag, men dersom misligholdet skyldes en hindring som ligger utenfor debitors kontroll, og som han ikke med rimelighet kan for-ventes å ha tatt i betraktning*

> *på avtaletiden, blir han fri for ansvar såfremt hindringen er av en slik karakter at det ikke med rimelighet kan ventes at han har kunnet unngå eller overvinne følgene av den («kontrollansvar»). For kjøp som omfattes av kjøpsloven, følger denne regel av kjøpsloven § 40 første og andre ledd, jf. § 27, og gjelder også individuelt bestemte forpliktelser. Dersom det ikke finnes særlig lovregulering, må ordningen med kontrollansvar også gjelde utenfor kjøpslovgivningens område, men slik at den på ulovfestet grunnlag bare gjelder for generisk bestemte forpliktelser, se Hagstrøm, op.cit. side 502 ff. Innenfor området for kjøpsloven gjelder det objektive ansvar bare direkte tap, se kjøpsloven § 40, jf. § 67. Hvis det ikke finnes særlig hjemmel for annet, må dette også antas å gjelde utenfor kjøpslovens område.*

Høyesterett uttaler i HR-2016-1235-A avsnitt 40 og 44 at:

> *For mitt føremål er det sentrale at hendinga må vere uventa og ekstraordinær, ho må verke inn utanfrå og ho må liggje utanfor partane sitt verkeområde. Nyansering må skje ut frå den konkrete kontraktsituasjonen og hendingsgangen. .....*
>
> *Dette er då også avgjerande for mi konkrete vurdering av om vilkåra for force majeure er oppfylte. Sjølv om vasstrykket kom utanfrå, var det etter sin art ikkje «en Ulykke ... udenfra» eller noko som «verkar inn utanfrå» og som var «sjeldsynt» eller «ekstraordinær». Snarare var det tale om forhold som ligg innanfor naturleg variasjon. Men først og fremst var årsaka til hendinga at røyret var underdimensjonert. Hydro hadde medvite valt dimensjonering for 100 meter vasstrykk, medan det i ettertid har vist seg at vasstrykket vart høgare. Og val av dimensjonar på røyret var i høgste grad noko som låg innanfor Hydro si kontrollsfære*

Retten finner det ikke sannsynliggjort at dataangrepet var upåregnelig og utenfor Nordlos kontroll. Retten viser her til at cyberangrep var en godt dokumentert og kommunisert trussel siden 2010-tallet. Nordlo var en profesjonell It-leverandør og det var gjentatte ganger gitt advarsler fra NSM (Nasjonal sikkerhetsmyndighet) både i 2017, 2019 og 2020 om faren for dataangrep.

I NOU 2018: 14 sikkerhet i alle ledd uttales det følgende:

> «*I Helhetlig IKT-risikobilde (2016) trekker NSM frem at underleverandører og kontraktører i økende grad blir utsatt for målrettede operasjoner. I tillegg er også tilfeldige systemer i tiltakende grad utsatt for kompromittering ved at de kan bli utnyttet for videre nettverksoperasjoner mot andre mål. Dette kan i prinsippet være et hvilket som helst IKT-system, som ikke er et mål i seg selv, men som fungerer som mellomledd mellom en angriper og det egentlige målet. Når det gjelder hvilke metoder som brukes i dag, slår NSM fast at mange digitale angrep innledes med bruk av ulike varianter av skadevare distribuert via e-post. Innhold og utforming fremstår som relevant og legitimt for mottakeren, men lenker og vedlegg inneholder skadelig kode som aktiveres ved at man klikker på lenken eller åpner vedlegget. NSM trekker også frem krypteringsvirus og innsidere som særlig aktuelle trusler.*»

Trusselaktøren som angrep Nordlo har vært aktiv siden 2018 og det legges ut fra forklaringene som ble gitt under hovedforhandlingen at dette var en aktør som var kjent i it-bransjen.

Retten kan således vanskelig se at det er var tale om et ekstraordinært eller upåregnelig angrep som ligger utenfor Nordlos kontroll og retten finner ikke at kontraktens pkt. 8 kommer til anvendelse.

Ansvarsgrunnlag

Btec har anført flere alternative grunnlag for ansvar. De har primært anfør at Nordlo er ansvarlig på culpagrunnlag. De har også anført kontrollansvar/gjennomgripende mangler som er så vesentlige at det er riktig å pålegge ansvar også uten hensyn til skyld og at Nordlo ha handlet grovt uaktsomt.

De samme anførslene er fremmet i forhold til disse. Retten finner på samme måte som Btecs egne prosessfullmektiger å behandle dem samlet da de samme hensyn gjør seg gjeldende ved vurderingen om Nordlo har opptrådt uaktsomt.

Ansvar forutsetter at Nordlo må kunne bebreides for sin opptreden og for ha hatt manglende sikkerhetsrutiner som har gjort det mulig for dataangriperne å få tilgang til Nordlos servere og deretter gjennomfør for dataangrepet som medførte at Btec mistet sine data.

Retten vil innledningsvis si noe om måten selve dataangrepet fant sted på.

Både EMP, Deloitte, Thorsheim og Defendable har foretatt vurderinger av datasikkerheten hos Nordlo. Det er imidlertid kun Atea som fysisk har gjennomgått serverne og kartlagt måten angrepet fant sted på.

Retten legger på bakgrunn av rapporten og vitneforklaringen til Geir Olav Skei i Atea til grunn at måten Nordlo ble utsatt for ransomware-angrepet ved var at trusselaktører logget seg inn på Nordlos nettverk via en såkalt «RD Gateway» som ledet til ax719rds, en terminalserveren tilhørende C. Påloggingen skjedde gjennom brukerkontoen til en av Nordlos kunder «post.hardmaler», som ikke krevde to faktorautorisering, fra Østerrike og Taiwan.

Det er ikke kjent hvordan trusselaktørene fikk tak i kundens påloggingsdetaljer. Ved hjelp av denne tilgangen ble det sluppet et såkalt «cobalt strike beacon» på serveren. Aktiviteten via dette beaconet er ukjent, men mye trolig er det benyttet til å tilegne seg administrasjonsrettigheter. Det er imidlertid ikke kjent hvordan trusselaktørene fikk tilgang til admistratorrettighetene. Det fremgår av Ateas rapport at til tross for at servere ax719rds hadde godt patchenivå på operativsystemet, så hadde serveren gammel usupportert, upatchet og utdarter programvare som kan ha blitt utnyttet.

Trusselaktørene gikk fra RD-serveren og opp til domenekontroller, og slapp ytterligere to «beacons» på ax167dc og ax13dc. Dette gjøres normalt for å lage flere veier til mål. Aktørene rekognoserte miljøet før de logget seg av ax719rds og hele miljøet kl. 0327. De benyttet flere administratorkontoer for det IT-ekspertene kaller «lateral movement», for eksekvering av Ryuk ransomware

Nest dag kl. 1900 dag logget trusselaktørene seg inn igjen og startet den innledende fasen av angrepet. De deployer en SOCKS_proxy (System BC) på ax13dc og slo av antivirus innebygd i Microsoft og hentet ut angrepsdata. Trusselaktørene detonerte så «Ryuk ransomware» både manuelt og automatisk på en håndfull servere. En egenskap ved «Ryuk ransomware» er at den sprer seg selv til øvrige systemer ved eksekvering. Angrepet har primært skjedd via ax13dc som har fungert som både staging- og jumpserver for trusselaktørene. De har jobbet parallelt med den automatiske Ryukspredningen for å manuelt igangsette krypteringsprosesser på servere der GPO for deaktivering av antivirus og/eller automatisert malware execution har feilet. Under angrepet ble det også introdusert ytterligere en versjon av Ryuk ransomware, med litt mindre filstørrelse, hvis bakgrunn og eventuelt detoneringspunkt er ukjent.

Hendelsen ble oppdaget av Nordlo sine systemer for overvåkning og varsling kort tid etter at angrepet ble iverksatt. Nordlo sitt personell stoppet angrepet og startet nedstengning av det rammede miljøet.

Det er i forbindelse med hendelsen i 2021 ikke gjennomført inngående analyser av hvordan angriperen har klart å få tilgang til Nordlos kontrollplan for administrasjon av infrastruktur og dette fremstår som uklart.

Det fremkommer at bruk av flerfaktorautentisering(MFA) var valgfritt for Nordlos kunder, og at det var flere kunder som ikke hadde tatt i bruk MFA.

Det kommer også frem av Ateas gjennomgang at i tillegg til Adobe Acrobat Reader DC versjon 2015.01020056 og Adobe Acrobat Pro DC versjon 2015.006.30527 som var end of support i april 2020, så var både Google Chrome (2019) og office-pakken (2018) upatchet og flere år gammel.

Det eksisterer ingen fullverdig oversikt over angrepets anatomi. Ransomware-angrep er ofte økonomisk motivert, og trusselaktørene jobber opportunistisk og går etter mål hvor de har stor sannsynlighet for å lykkes.

Hvilke sikkerhetstiltak og -systemer som kan forventes, må ses i lys av hva Btec som ASP-kunde har kjøpt og betalt for. Det er på det rene at det her er kjøpt en ordinær ASP-løsning og ikke noe ekstra sikkerhetspakke.

Retten legger ut fra den samlede bevisførselen til grunn at hele prinsippet for ASP er at flere kunder deler fysisk infrastruktur som servere, brannmurer, backupløsninger etc. for å oppnå en kostnadseffektiv it-leveranse. Selv om man deler fysisk infrastruktur, bør man skille kundene fra hverandre logisk. Dette ble gjerne gjort ved å dele hver kunde i eget Organizational Unit (OU) i Active Directory (AD). Denne måten å skille kunder på betyr at flere kunder deler samme AD. Dette er en risiko ved cyberhendelser fordi en aktør som klarer å skaffe seg administratorrettigheter vil få dette på tvers av alle kunder i samme AD.

Segmentering er et vanlig begrep innen IT. I hovedsak benyttes begrepet om å skille ulike miljøer fra hverandre i egne logiske nettverk og evt. også i egne domener. Som regel segmenterer man ut fra en risikovurdering. Det er vanlig å skille ut et eget management nett (også kalt backbone, administrasjonsplan) I dette nettet ligger ofte underliggende infrastruktur som virtualiseringsplattform, administrasjonsservere, nettverksutstyr etc. Noen

velger også å legge backupservere i management nettet mens andre velger å legge backupservere i et eget dedikert backupnett.

Btec fikk levert et program ved navn Autocalc via sin ASP-løsning. Ved leveranse av programvare utover standardprogramvare er det vanlig at programvareleverandøren deltar under installasjonen for å sikre at programvaren blir installert etter beste praksis. Programvareleverandøren gjennomførte installasjonen med støtte fra Nordlo. Autocalc ble da konfigurert til å lagre data direkte på Terminalserveren. Dette viste seg senere å bli relevant for Btec sitt tap av data, fordi backupserveren som tok backup av terminalservere ikke var segmentert til managementnettet enda.

***

Overordnet er spørsmålet om Nordlo har handlet uaktsomt ved ikke å ha sikret seg bedre mot dataangrep og hatt bedre rutiner for å sikre backup av Btecs data.

Slike unnlatelser kan en dataleverandør blir ansvarlige for. Men forutsetningen må være at det forelå en særskilt oppfordring til å handle.

Sentralt i vurderingen er om Nordlo har brutt relevante regler eller bransjenormer og om eventuelle tiltak ville ha kunne forhindret skaden.

NSM (Nasjonal sikkerhetsmyndighet) har utarbeidet grunnprinsipper for IKT-sikkerhet. Det var versjon 1 og 2 av denne fra hhv 2017 og 2020. Det er der gitt en beskrivelse av hva virksomhetene skal sikre seg mot og hvorfor virksomheter skal sikre et IKT-system. Prinsippene er inndelt i fire hovedområder: identifisere/kartlegge, beskytte/opprettholde, oppdager og håndtere/gjenopprette. De mest sentrale grunnprinsippene er som følger: NSM grunnprinsipp 1.1 – «Kartlegg styringsstruktur, leveranser og understøttende systemer». Sentralt for helhetlig arbeid med sikkerhetsstyring er å identifisere og implementere en strategi, strukturer og prosesser på sikkerhetsstyring. NSM grunnprinsipp 2.2 – «Etabler en sikker IKT infrastruktur». Fastslår at det bør etableres en helhetlig sikkerhetsarkitektur. NSM pkt. 2.2.3, 2.2.4 og 2.2.5 nettverkssegmentering. Virksomheten skal gjennomføre nettverkssegmentering. NSM pkt. 2.2.6 tilgangsstyring. Virksomheten skal regulere tilgang til sine tjenester. NSM grunnprinsipp 2.4 – «Beskytt virksomhetens nettverk» Virksomheten skal kontrollere og beskytte nettverkene sine mot interne og eksterne trusler. NSM pkt. 2.4.1 endepunktsikkerhet Overvåking og sikring av endepunkter. NSM grunnprinsipp 2.5 – «Kontroller dataflyt» Virksomheten skal ha kontroll på informasjons mellom ulike deler av systemer. NSM grunnprinsipp 2.6 – «Ha kontroll på identiteter og tilganger». NSM grunnsprinipp 2.9 – «Etabler evne til gjenoppretting av data. NSM grunnprinsipp 3.2 – «Etabler evne til sikkerhetsovervåkning».

I følge sakkyndig vitne Thorsheim var det alvorlige mangler i forhold til de forventninger en har til denne type driftsmiljø. Han pekte bl.a. på manglende tofaktorautenisering, manglende regionsperre, manglende oppdatering av programmer og manglende løsning for sikkerhetskopiering/backup. Ifølge Thorsheim er det er allment kjent at usupportert og utdatert programvare, samt manglende sikkerhetsoppdateringer til gjeldende programvare, utgjør en kjent og reell fare. Nasjonal Sikkerhetsmyndighet sine «Grunnprinsipper for IKT-sikkerhet», i likhet med det meste kan man finne av krav, retningslinjer og anbefalinger innen it-sikkerhet, er svært tydelige på at programvare må holdes oppdatert, og at programvareoppdateringer («patcher») installeres så fort som mulig.

I følge sakkyndig vitne i Deloitte Strangstad er store mangler i hvordan Nordlo har jobbet proaktivt med å identifisere, kartlegge, håndtere og rapportere risiko. Angrepet i 2021 utnyttet en rekke svakheter og sårbarheter i Nordlos infrastruktur, blant annet:

> (1) Mangel på bruk av flerfaktorautentisering for brukere gjør det enkelt for en angriper å overta kontroll på brukeridentiteter, da det er tilstrekkelig å kun ha brukernavn og passord.
>
> (2) Valgfri bruk av flerfaktorautentisering hos kunder medfører at valg som tas av enkelte kunder av Nordlo påfører høy risiko for andre kunder av Nordlo uten at disse er kjent med denne risiko.
>
> (3) Svak segregering mellom brukerplan og kontrollplan gjorde det mulig for angriper å forflytte seg fra en vanlig brukerkonto, ta over administrative brukere, og helt eller delvis overta kontroll over Nordlos infrastruktur.
>
> (4) Mangel på bruk av flerfaktorautentisering for administrative kontoer gjør det enkelt for angriper å overta kontroll på administrative kontoer, da angriper ikke blir utfordret med flere verifiseringer av identitet.

(5) Mulig mangelfull logginnsamling og evne til å oppdage trusler medførte at hendelsen ikke ble oppdaget i en tidlig fase, og angriperen kunne fortsette sin operasjon uforhindret og i det skjulte.

(6) Mangelfull segregering mellom kundenett medførte at angriper enkelt kunne påføre skade på tvers av hele Nordlo sin kundeportefølje.

(7) Feil konfigurering av sikkerhetskopiering medførte at Btec sine data ikke ble sikkerhetskopiert til et sikkert område.

(8) Mangelfull test av sikkerhetskopiering og rutiner for gjenoppretting medførte at feilkonfigurering av sikkerhetskopiering ikke ble oppdaget. Deloitte har vurdert at dette er sårbarheter som burde og kunne ha vært håndtert gjennom god etterlevelse av NSM sine grunnprinsipper for IKT-sikkerhet, eller tilsvarende rammeverk/standarder for god-praksis.

Defendable har i sin rapport og under forklaringen til H trukket frem at Defendable mener at hendelsen trolig reelt startet på et tidligere tidspunkt enn det som legges frem i hendelsesrapporten til Atea. I rapporten er det ikke avdekket rotårsaken til hvordan trusselaktøren tilegnet seg den initiale tilgangen. Analysearbeidet fremstår som overfladisk utført. For Defendable er det heller ikke mulig å stadfeste når hendelsen startet, men basert på erfaring med lignende hendelser så kan det være snakk om alt fra dager til år. Som følge av den informasjonen som foreligger, blant annet Ateas rapport etter hendelsen, er det Defendables syn at det er vesentlige mangler på flere områder:

- Ingen moderne endepunktsikring (EDR/XDR)
- Svært svak tilgangskontroll (mangelfull flerfaktor-autentisering)
- Svært svak kontroll over nettverkstrafikk inn og ut av kritiske systemer
- Svak kontroll over endepunkter
- Svak kontroll rundt oppdateringer av programvare
- Unødvendig bruk av for høye rettigheter og som enkelt kan misbrukes (domeneadministrator)
- Mangelfull logging og overvåking av kritiske systemer
- Dårlige sikkerhetskopieringsrutiner
- Manglende segmentering og skille mellom Nordlos operativt nettverk og kunder nettverk

Retten legger ut fra partsforklaringen til D i Nordlo til grunn at det i liten grad forelå skriftlige rutiner i selskapet knyttet opp mot sikkerhet og sårbarhetsanalyser rundt kundene. Dette fremstår som en svakhet slik retten vurderer det og noe en burde kunne forvente av en it-leverandør med 1100 ulike servere og ca. 250 kunder. Når en holder dette opp mot det faktum at det heller ikke foreligger noen skriftlig avtale mellom Btec og Nordlo fremstår dette som noe symptomatisk for måten selskapet ble drevet på. Det fremstår i stor grad som om Nordlo var opptatt av å etablere løsninger uten at dette var nedfelt i noen skriftlige rutiner rundt dette. De fremgikk også av hans forklaring at en flere av sikkerhetstiltakene var retter opp mot driftsstans av andre årsaker enn cyberangrep. Samtidig finner retten det ikke sannsynliggjort at dette er ensbetydende med at cybersikkerheten ikke ble ivaretatt i selskapet.

Det er etter rettens syn ikke tvilsomt at en av Nordlos hovedforpliktelser etter avtalen var å tilby saksøkerne en dataløsning som ivaretok den nødvendige sikkerhet mot bl.a. cyberangrep. Det må stilles strenge krav til IT-leverandørens egne sikkerhetstiltak, da et angrep vil være svært kritisk for Nordlo selv og ikke minst også for kundenes virksomheter

Retten finner at selv om det foreligger noen løsninger som ikke er helt optimale er det ikke sannsynliggjort at Nordlo handlet uaktsomt.

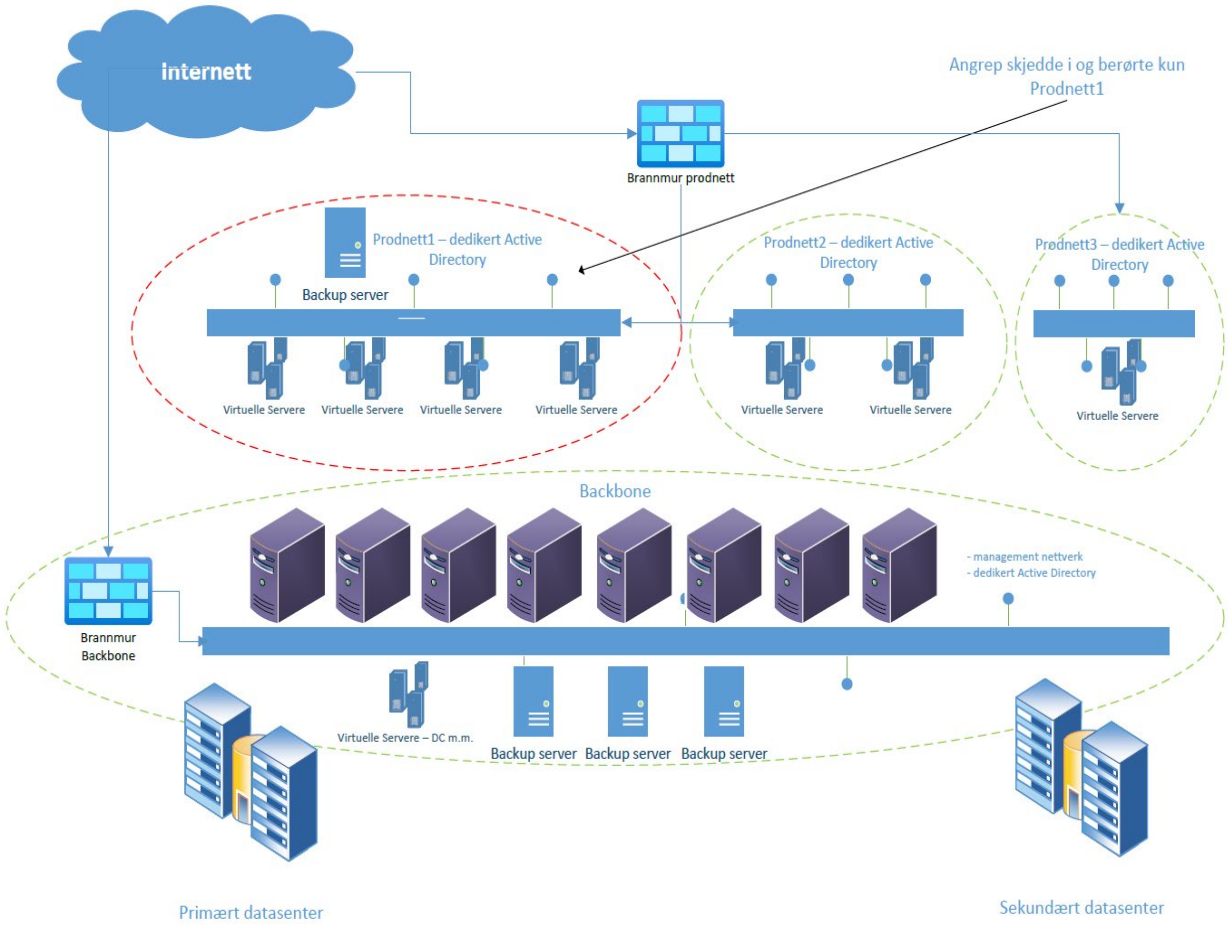
Etter den samlede bevisførselen og partsforklaringen til D må det legges til grunn at Nordlo hadde implementert en rekke tiltak for å redusere risikoen for sikkerhetshendelser selv om disse ikke var nedfelt i noen skriftlige rutiner.

Det ble benyttet to datasenter hvor kundeservere og kritisk infrastruktur var delt mellom disse. Datasentrene hadde gode løsninger innen strøm, kjøling og nettverk. Det ble tatt daglig backup fra begge datasenter. Backup ble tatt til «motsatt datasenter» for å skille backup fysisk fra produksjon. Nordlo hadde segmentert ut det meste av kritisk infrastruktur inkludert backup i eget nett. Dette nettet (backbone, managementnett, administrasjonsplan) hadde eget domene og følgelig også egne brukerkontoer. Managementnettet ble aldri rammet av angrepet og segmenteringen fungerte altså etter hensikten.5. Nordlo hadde segmentert kunder i 3

ulike prodnett. (Flest kunder på prodnett1 som ble rammet) Nordlo benyttet MFA på alle kontoer i management nettet. Det var installert antivirus på alle servere. Det var implementert brannmur som et sikkerhetslag. Det var rutiner for oppdatering av operativsystem på serverne.

Retten finner det sannsynliggjort at Nordlo var opptatt av segmentering. De hadde i 2019 startet arbeidet med å segmentere de ulike nettene nettopp for å sikre kundene sine.

Nordlo har utarbeidet en nettveksskisse som illustrerer oppbygningen:



Nordlo sitt IT-miljø bestod på angrepstidspunktet av 4 segmenterte nett. Dette var Prodnett 1-3 samt management nett (backbone). De fire nettene var skilt på nettverksnivå og hadde også hvert sitt domene med egne domenekontrollere og følgelig egne brukerkontoer. Det var Prodnett1 som ble rammet av angrepet. Prodnett2, Prodnett3 og Managementnett ble ikke rammet.

I utgangspunktet lå all backup lagret på servere i Managementnettet, som ikke be rammet. Imidlertid var det en backupserver igjen i Prodnett1 som enda ikke var flyttet over til Managementnettet. Dette var en backupserver som tok backup av Terminalserverne i Prodnett1 som kundene benyttet for å bruke ASP-tjenesten. Slike servere inneholder normalt kun operativsystem og programvare, men ikke kundefiler. Backup av disse serverne hadde derfor lavere risiko enn backup av filserverne og det var årsaken til at denne backupserveren ble prioritert å flytte til sist. Tap av terminalserverne inkl. backup vil normalt ikke gi tap av kundens data, men potensielt kunne gi noe merarbeid med å måtte reinstallere serveren.

Nordlo benyttet to datasenter for å levere ASP-tjenesten. Det var servere for både drift og backup i begge datasentrene. Backup var konfigurert slik at produksjon som ble levert fra det ene datasenteret hadde backup sin plassert i det andre datasenteret. Dette var et tiltak for å hindre at en fysisk hendelse som brann eller vannskade skulle kunne ramme både produksjon og backup samtidig.

Det ble tatt daglig backup av løsningen til Btec som avtalt. Btec hadde ingen databaseløsning og benyttet kun filserver for lagring. Det ble tatt backup av filserver hver dag og denne backupen ble lagret på i motsatt datasenter av produksjon og i det segmenterte backbonenettet som også hadde eget domene.

Btec fikk etter hendelsen gjenopprettet all data som hadde vært lagret på filserveren. Dette fordi angriperne aldri klarte å bevege seg over til backbone nettet selv med full kontroll på produksjonsnettet. Løsningen fungerte altså etter hensikten ved å sikre at backup var utilgjengelig for angriperen.

Nordlo og tidligere Appex hadde opprinnelig en flat nettverksstruktur der alt ble samlet i samme nett. Nordlo hadde allerede tatt grep da dataangrepet startet. Nordlo var i ferd med å etablere en bedre segmentering. Dette viser slik retten vurderer det at Nordlo var opptatt av å følge Nasjonal sikkerhetsmyndighets råd om å sikre segmentering og at de fulgte med på det økende trusselbildet med hackerangrep og den sårbarheten som ligger ved å ha flere kunder i en ASP-løsning.

Det faktum at Prodnett2, Prodnett3 og Managementnett ikke ble rammet, tyder slik retten vurderer det på at segmenteringen har fungert etter hensikten. Det faktum at angriperne ikke klarte å bevege seg over til backbone nettet selv med full kontroll på produksjonsnettet viser også at segmenteringen og løsninger fungerte etter hensikten ved å sikre at backup var utilgjengelig for angriperen.

Sikkerhetskopier på et eget nettverk som var fysisk atskilt fra det andre datasystemet ville hindret eller redusert konsekvensene av cyberangrepet betraktelig. Nordlo hadde 1100 servere. Sikkerhetsarbeid er en kontinuerlig prosess som tar tid og krever ressurser. Nordlo Haugesund er en mindre IT-bedrift med 13 ansatte og det er da påregnelig at en slik prosess tar noe tid. Nordlo hadde ikke kommet så langt i prosessen at de hadde fått segmentert ut den siste backupserveren som tok backup av terminalserverne. At Nordlo hadde latt denne være den siste delen de segmenterte hadde sin årsak i at kritisk data normalt ikke ble lagret på terminalserverne. Retten kan således ikke se at det er grunnlag for å kritisere Nordlo at de under en prosess der de er i ferd med å sikre kundene bedre i tråd med de anbefalinger som kom fra Nasjonal sikkerhetsmyndighet, foretok en prioritering av hvilke servere de segmentert ut først.

Retten viser her til Ateas rapport om evaluering av hendelsen hvor det fremkommer følgende:

> *«Det var allerede påstartet en flyttejobb hvor målsetningen var å få infrastruktur- og backup-tjenester ut fra ASP-nettet og over i ett eget nett dedikert til infrastruktur i forkanten av hendelsen. På bakgrunn av denne flyttejobben hadde Nordlo allerede etablert gode og segmentert backup og tap av servere med assosiert data var minimal.»*

Nordlo foretok sikkerhetskopier i tråd med avtalen. Det har blitt gjennomført sikkerhetskopier av begge Btecs servere, RDS- serveren(ax1061rds) og filserveren(ax1062file). Dataene som var tatt backup fra filserveren ble gjenopprettet etter angrepet og tilbakelevert Nordlo.

Btec fikk etter at de gikk over til en ASP-løsning installert Autocalc. Programvare som Autocalc har som regel behov for en database for kunne lagre data. Programvareleverandøren Sigma deltok under installasjonen. Autocalc ble da konfigurert til å lagre data direkte på Terminalserveren. Dette viste seg senere å bli avgjørende for Btecs tap av data, fordi backupserveren som tok backup av terminalservere ikke var segmentert til managementnettet enda. Denne serveren ble prioritert å segmentere til slutt fordi det skulle være lav risiko knyttet til dataene som lå på denne serveren.

Det sakkyndige vitnet fra Deloite, Strangstad, har anført at mangelfull test av sikkerhetskopiering og rutiner for gjenoppretting medførte at feilkonfigurering av sikkerhetskopiering ikke ble oppdaget. Deloitte har vurdert at dette er sårbarheter som burde og kunne ha vært håndtert.

Selv om det er en svakhet at konfigureringen ble satt opp slik, og trolig er hovedårsaken til at dataene ikke lot seg gjenopprette, kan retten her ikke se at dette utelukkende kan lastes Nordlo. Som angitt ovenfor er Nordlo Haugesund en relativt liten IT-bedrift. De hadde 1100 servere med ca. 250 kunder, der hver kunde kunne ha opptil flere hundre brukere.

Selv om Nordlo opererer i IT-bransjen, kan det ikke forventes at de har inngående kjennskap til ulike spesialprogrammer som blir benyttet hos de ulike kundene/bransjene og hvordan disse er bygget opp. Ifølge D hadde han ikke noe kjennskap til Autocalc. Han hadde ikke noe kjennskap til at det inneholdt noe virksomhetskritisk data. Btec var selv nærmest til å orientere Nordlo om at det lå virksomhetskritisk data på Autocalc. Nordlo hadde således ikke noen oppfordring til å undersøke om det var foretatt noen feilkonfigurering som gjorde at data ble lagret direkte på terminalserveren og ikke filserveren slik det burde ved virksomhetskritisk data.

Nordlo hadde således ikke noen særskilt oppfordring til å være særskilt oppmerksom på at det her lå virksomhetskritisk data som var særlig sårbar da de valgte å prioritere backupserveren som tok backup av

terminalservere til slutt. Hadde Nordlo hatt en slik informasjon, hadde de hatt en særlig oppfordring til å også ha fokus på data som var lagret på terminalserver. Slik retten vurderer det er Btec den nærmeste til å bære risikoen når de lagrer på terminalserver istedenfor filserveren som gir en mye større sikkerhet.

Hvilke krav som skal stilles til Nordlos tjeneste må også vurderes opp mot hvilke tjeneste Btec har bestilt og betalt for. Btec har bestilt en ordinær ASP-løsning. Nordlo har ikke markedsført seg som noen sikkerhets bedrift og det var heller ikke en sikkerhetstjeneste som ble tilbudt Btec. Btec bestilte en ordinær ASP-løsning.

Selv om Nordlo Norge er ISO-sertifisert så er ikke Nordlo Haugesund det. De har aldri markedsført seg med dette.

Det ble daglig tatt backup av kundenes data og månedlig backup for langtidslagring. Det var ifølge D daglige rutiner for sjekk av brannmur, backup osv. De hadde automatisk overvåkning og varsling ved spesielle hendelser eller problemer med tjenestene.

Retten vil bemerke at det har skjedd en betydelig profesjonalisering innen dataangrep som ved ransomware, hvor godt organiserte kriminelle aktører bryter seg inn i dataservere til myndigheter, bedrifter, organisasjoner mv, krypterer data og krever store løsepengesummer i kryptovaluta for å gi den rammede sine data tilbake.

Det vil alltid oppstå sikkerhetshull som profesjonelle hackere vil kunne finne og utnytte for å komme seg inn på datasystemer, og for å være best mulig rustet mot angrep må data-systemene ha de til enhver tid siste sikkerhetsoppdateringene fra programvareleverandørene og ha de nødvendige preventive tiltak.

Hackerne fikk ifølge sakkyndig vitne Skei inngang til datasystemets driftsmiljø ved å bruke en kundes brukernavn og passord som var på avveie.

Det er enighet mellom de sakkyndige at tofaktorautentisering (MFA) er et enkelt preventivt tiltak som i stor grad vil kunne vanskeliggjøre et dataangrep.

Nordlo benyttet MFA på brukerkontoer i Managementnettet. Nordlo har således tatt grep for å sikre de mest kritiske dataene. For kunder på ASP-løsningen hos Nordlo var det imidlertid valgfritt med MFA. Det medførte at det i samme nett var noen kunder som benyttet MFA og noen som ikke gjorde det. Dette gjorde at kunder som hadde valgt MFA hadde samme risiko som kunder som hadde valgt bort MFA.

Det har fra Btec blitt trukket frem at Nordlo ikke informerte om farene og sårbarhetene og at hadde de det ville de selv kunne ha satt i verk sikkerhetstiltak. Retten finner at de vanskelig kan høres med dette. Btec har selv valgt å ikke møte opp til på to møter de var innkalt til før tjenesten ble tatt i bruk. De må da selv bære risikoen for at de ikke fikk denne type informasjon.

Nordlo kunne krevd at alle kundene brukte MFA for å redusere risikoen for angrep.

Btec hadde selv valgt å ikke benytte MFA og retten er enig med sakkyndig Espedal om at de dermed ikke var på en høyere plattform enn Btec selv hadde valgt.

Selv om MFA var svært utbredt i bransjen for å høyne sikkerhetsnivået, var dette noe flere andre dataleverandører også hadde som et frivillig tiltak. Ifølge sakkyndig vitne Espedal i EMP Secure måtte brukere hos Microsoft frem til 2019 selv aktivt velge å aktivere MFA dersom de ønsket dette. Fra oktober 2019 ble krav om MFA innført ved å sette «Security Defaults» som standard for alle nye M365 kunder. Det var imidlertid ikke før i januar 2025 at Microsoft gjennomførte dette som krav for eksisterende kunder. Fremdeles er ikke MFA krav fullført på alle områder pr mai 2025. Google har ifølge Espedal pr mai 2025 heller ikke implementert tvungen MFA, men planlegger dette i løpet av 2025. Retten kan således vanskelig si at Nordlo, som en mindre IT-leverandør, har opptrådt klanderverdig ved ikke å pålegge brukerne tvungen MFA i 2021 når store aktører som Google og Microsoft heller ikke hadde som pålegg til eksisterende kunder. Nordlo hadde dette som et frivillig tiltak.

Trusselaktøren logget seg på via Taiwan og Østerrike. Det å bruke geografiske begrensninger ifht fra hvilke land pålogging kan skje vil kunne hindre eller forsinke en angriper, selv om det dog ikke kreves så gode data-kunnskaper for unngå dette eksempelvis ved å bruke proxyserver som er lokalisert i Norge. En geosperre vil unne vanskeliggjøre en angriper, men retten kan vanskelig se at Nordlo kan klandres for å ikke ha innført dette. Nordlo har en rekke kunder som blant annet arbeider opp mot offshore og skipsbransjen og der de reiser mye i jobbsammenheng og der kunden og deres brukere således har behov for å logge seg på fra utlandet.

Ryukviruset, som er benyttet i denne saken, knyttes til internasjonal organisert kriminalitet. I følge sakkyndig Skei i Atea er Ryuk en tett gruppering som har samarbeidspartnere som tas seg inn til ofrene og de deler utbytte

med samarbeidspartnerne. Gjennomsnittlig utbetaling i 2021 var 700 000 dollar. Det ble rapportert om 20 ofre pr uke i 2020 og det er en stor organisasjon. De hadde 1 milliard dollar i løsepenger i 2020. De angriper alle mål. I 2023 angrep de blant annet Coop, Tomra, Avant, teknett og Eurosko. I følge Skeie angriper de både små og store bedrifter. Selv om det er advart mot disse er det fortsatt flere store bedrifter som blir tatt. Det siste store angrepet var mot datafirmaet Every i Sverige. Dette er et stor IT-selskap med langt større ressurser til sikkerhetstiltak enn Nordlo Haugesund.

Det ble her benyttet cobalt strike beacon under dataangrepet, Dette er ifølge sakkyndig Skei et rammeverk som trusselaktørene bruker for å angripe servere eller nettverk. De kommer inn og planter dette. Det brukes som en mellomstasjon for å sende informasjon videre. Patchenivået på operativssytemet var godt. Det er høyst uklart hvordan trusselaktørene fikk tilgang til adminstatorrettighetene. Det er således slik retten ser det ikke mulig for retten å kunne konstatere hvilke sårbarheter som ble utnyttet og i hvilken grad Nordlo har unnlatt å iverksette tiltak som ville ha kunne forhindre angrepet og om de således har handlet uaktsomt.

Det har fra Btec blitt anført at det forelå mangelfull overvåkning og at angrepet burde vært avdekket på et tidligere tidspunkt da de tok seg inn og således forhindret selve angrepet.

Retten kan heller ikke gjennom bevisførselen se at det er sannsynliggjort at angriperne har angrepet på et tidligere tidspunkt enn angitt i Ateas rapport. Defendable har anført at angrepet trolig ble gjennomført flere måneder på forhånd. Retten kan ikke se at denne påstanden er underbygget av noen bevis i saken og baserer seg etter det retten oppfatter kun på antakelser. Retten kan således ikke se at det er ført bevist for at dette var et angrep på et mye tidligere tidspunkt. Defendable har ikke selv foretatt egne undersøkelser og baserer seg på Ateas undersøkelser der det ble konstatert at angriperne kom inn dagen før angrepet ble iverksatt.

Det har fra Betecs sakkyndige vitner blitt anført at Nordlo ikke hadde tilfredsstillende sikkerhetsovervåkning. Det har blitt anført at det burde vært installert automatisk overvåkning som i større grad overvåket datasikkerhet og ikke bare driftssikkerhet og at en da ville ha kunne forhindret dataangrepet. Sakkyndig vitnet Strangstad i Deloite anslo i retten at mange it-firmaet enten gjør det selv eller setter det ut til andre. Strangstad anslo i retten at dette var kostbart og anslo årlige driftskostnader til på 5 millioner for en slik automatisk sikkerhetsovervåkning, i tillegg kommer kostnader med å installere det. Dersom en skal gjøre det internt må en for å ha en effektiv overvåkning har 24-7 tjeneste som vil kreve 8-10 ansatte som går skift.

Tjenesten Nordlo leverer er ikke en sikkerhetstjeneste og retten kan ikke se at det med rimelighet kan forventes at et lite IT-firma skal sette inn så store ressurser på overvåkning.

Det må her legges betydelig vekt på profesjonaliteten av angrepet. Der både antivirusprogrammet og varslinger ble slått av under angrepet.

D forklarte i retten at de hadde overvåkingssystemer som oppdaget angrepet og at de umiddelbart iverksatte tiltak som begrenset angrepet. Det er også bekreftet av Atea at Nordlo allerede hadde igangsatt strakstiltak og anbefalinger.

Det fremgår av Anders Strangstad i Deloittes sakkyndige rapport av 04.11.2024:

> *Det at et cyberangrep faktisk fant sted, er ikke nødvendigvis en direkte indikasjon på mangelfulle sikkerhetsrutiner. Cyberangrepene utvikler seg stadig, og dagens trusselbilde er mer komplekst enn noen gang. En organisasjon kan ha moderne sikkerhetstiltak på plass, men avanserte og sofistikerte angrep kan fortsatt finne veier gjennom eksisterende forsvar.*

Dette er også bekreftet av sakkyndig Skei. Dataangriperne har tilegnet seg brukernavn og passord på en høyere nivå. Ifølge Skei er det mer enn 200 mulige måter å gjøre dette på. Sertifiseringer, tjenester på serveren kan utnyttes, feilkonfigurering mm blir benyttet. Ifølge Skei er listen over måten å gjøre dette på svært lang. Det er kun unntaksvis at trusselaktørene ikke har klart å eskalere i løpet av noen få timer. De klarer ifølge Skei som regel det når de har kommet seg inn. Retten finner således ikke å legge avgjørende vekt på anførselen om unødvendig bruk av for høye rettigheter og som enkelt kan misbrukes av domeneadministratorene.

Skei i Atea har ingen bindinger til noen av partene og er engasjert på vegne av Tryg forsikring. Retten finner således å tillegge hans vurdering stor vekt.

Det er på det rene at det ble avdekket programvarer som var utdatert og dette er en svakhet som en ofte ser at trusselaktørene benytter seg av og Nordlo burde hatt bedre systemer for å fange opp dette.

Retten legger til grunn at dataangrepet mot Nordlo ble utført av godt organiserte utenlandske kriminelle med svært høy teknologisk kompetanse. Selv om sikkerhetstiltak som tofaktorautentisering kunne vært iverksatt og oppdatering av programvarer var utdatert er det svært vanskelig å verne seg mot denne type datakriminalitet, og det er rettens oppfatning at det var deres profesjonalitet som var årsaken til at de klarte å ramme Nordlo i en slik grad som de gjorde. Selv om det er påpekt enkelte sårbarheter i Nordlos datasystem vurderer retten bevisene slik at Nordlo har hatt fokus på og hatt god nok datasikkerhet.

Hackerne kom seg som nevnt inn på datasystemet via brukernavn og passord på avveie. Hackerne logget seg på og foretok en del rekognosering for å kartlegge nettverket, tok ut data og logget av. De var så borte i 15 timer før de logget på igjen på kvelden. De gikk inn via fjernstyringsverktøy via samme domenekontroller som tidligere og slo av antivirus innebygd i Windows, før de deretter detonerte «Ransomware» både manuelt og automatisk på en del servere, som spredde seg via serverne. Serverne ble låst og filer kryptert. D var på vakt og fikk opp varsler om at filer var kryptert, og forstod da med en gang at de med stor sikkerhet var angrepet. Han stengte datasenteret i løpet av minutter ved at strømforsyningen ble slått av. Intern varsling ble sendt ut og det ble satt krisestab. Kunder ble varslet, og arbeidet med gjenoppretting ble startet og pågikk gjennom helgen. Skei forklarte at Nordlo var veldig godt i gang med gjenoppretting og hadde ifølge ham kontroll da Atea kom inn i bildet noen dager etter angrepet.

Når det gjelder en av hovedforpliktelsene til Nordlo, nemlig å sikre backup for kundene, følger det av avtalen at Nordlo skulle ta sikkerhetskopi av kundens data flere ganger daglig og at sikkerhetskopier skulle oppbevares i annen bygning en datasentralen. Dette ble overholdt av Nordlo. Videre skulle Nordlo etter avtalen på kundens forespørsel tilbake-kopiere angitte data fra siste sikkerhetskopi. Nedetiden var lang for Btec og de fikk aldri dataene sine tilbake. Da hackerangrepet skjedde hadde Nordlo påbegynt, og nær fullført, arbeidet med å flytte ut backup i eget nettverk, altså fysisk server i eget nett frikoblet «produksjonsområdet», for å bedre sikkerheten ytterligere. Om Nordlo hadde vært ferdig med arbeidet, hadde de antakelig ikke opplevd de konsekvensene som de gjorde, at de ble mer begrenset. Kun 4 av 250 kunder mistet data, noe som slik retten vurderer det viser at sikkerhetssystemene har fungert.

Det er ikke tvilsomt at Btec ble svært hardt rammet ved hackerangrepet, og at de hadde lang nedetid som gikk ut over deres omsetning. At Btec mistet alle sine data var det mest kritiske og de har senere blitt påført økonomisk tap som følge av dette.

Det er som sagt rettens oppfatning at Nordlo hadde tilstrekkelig og god sikkerhet, og at det må hensyntas at misligholdet er en følge av et målrettet dataangrep fra utenlandske profesjonelle aktører. Det er riktig at Nordlo hadde et ansvar for å ivareta sikkerheten, men dette innebærer ikke at også saksøkerne selv har et ansvar for å vurdere hva som kan bli følgene av et dataangrep mot datasystemet de er en del av. Ingen kan til enhver tid garantere 100 % for sikkerheten på et datasystem, og avtalen er som nevnt klar på Nordlos begrensede ansvar og at det er kundens ansvar å benytte seg av muligheten til å forsikre sine data.

Slik retten ser det har Nordlo ikke handlet uaktsomt. Saksøkers anførsler om grov uaktsomhet og at utfylling av avtalen faller bort som følge av grov skyld og lojalitetsbrudd kan heller ikke føre frem. For at en handlemåte skal kunne karakteriseres som grovt uaktsom må denne representere et markert avvik fra vanlig forsvarlig handlemåte, jf. bl.a. Rt-1989-1318 (advokatansvar). Retten kan ikke se at det er tilfelle og viser til de samme drøftinger som ovenfor.

Retten kan heller ikke se at Nordlo kan anses for å være ansvarlig ut fra et kontrollansvar.

Høyesterett har HR-2022-192-A uttalt følgende om kontrollansvaret:

> *Oppsummeringsvis legger jeg etter dette til grunn at vilkåret om at årsaken til mangelen må ligge utenfor selskapets kontroll, må vurderes konkret. Det avgjørende er om årsaken ligger innenfor det selgeren – etter en objektiv vurdering – kunne kontrollere eller påvirke gjennom planlegging, styring og kontroll med virksomheten. Foreligger det handlingsalternativer for selger som ville ha forhindret årsaken til mangelen, ligger årsaken normalt innenfor selgers kontroll, med mindre årsaken skyldes ekstraordinære forhold. Det er ikke avgjørende om selgeren har opptrådt aktsomt.*

De samme hensyn gjør seg gjeldende her som ovenfor under culpavurderingen.

Dataangrepet mot Nordlo ble utført av godt organiserte utenlandske kriminelle med svært høy teknologisk kompetanse. Selv om sikkerhetstiltak som tofaktorautentisering kunne vært iverksatt og oppdatering av programvarer var utdatert, er det svært vanskelig å verne seg mot denne type datakriminalitet, og det er rettens

oppfatning at det var deres profesjonalitet som var årsaken til at de klarte å ramme Nordlo i en slik grad som de gjorde. Dataangrepet må således etter en konkret vurdering anses for å ligge utenfor Nordlos kontroll selv om forholdet ikke kan anses for å være et Force Majeure tilfelle.

Nordlo blir etter dett å frifinne for erstatningsansvar etter culpa, grov uaktsomhet og kontrollansvar.

Konklusjon

Btec er bundet av Nordlos standardkontrakt. Nordlo kan ikke anses å være ansvarlig for Btecs økonomiske tap på grunnlag av culpa, grov uaktsomhet eller kontrollansvar.

Det er på det rene at Nordlo som følge av dataangrepet misligholdt sin del av kontrakten ved at de ikke klarte å sørge for tilgjengelighet og at det tok noe tid før Btec fikk tilgang til ASP-tjenesten igjen. Nordlo tok backup, men Btec tapte data som var lagret i Autocalc.

Retten finner det gjennom partsforklaringen til A og gjennomgangen til I i Defendable og J sannsynliggjort at Btec har lidd et betydelig økonomisk tap som følge av dataangrepet. Retten finner det ikke nødvendig å gå inn på størrelsen av dette på grunn av de ansvarsbegrensninger som fremgår av kontrakten.

Hensett til at Btec må anses for å være bundet av ansvarsbegrensningene i standardkontrakten til Nordlo finner retten at Nordlo kun er erstatningsansvarlig for Btecs direkte tap innenfor rammen av 3 månedsleier. Månedsleien var kr. 2760,– pr måned. Nordlo dømmes etter dette til å betale til Btec kr. 8280,–

Sakskostnader:

Det følger av tvisteloven §20-2 første ledd at en part som har vunnet saken har krav på full erstatning for sine sakskostnader fra motparten. Saken er vunnet hvis parten har fått medhold fullt ut eller i det vesentlige, jf. tvl. §20-2 andre ledd.

I Rettsdatas kommentarer til bestemmelsen fremgår det at:

> «*Medhold «i det vesentlige» er oppnådd når resultatet for parten er så gunstig at mot-parten ikke har oppnådd noe av betydning sammenholdt med det som ville vært situasjonen om motparten hadde akseptert den vinnende parts standpunkt fullt ut før sak ble reist. Parten har da nådd frem på vesentlige punkter. Tilsvarende vil gjelde dersom motparten taper saken praktisk talt fullt ut, bortsett fra å ha fått medhold på et mindre vesentlig punkt. Forarbeidene nevner som eksempel en erstatningssak som omhandler en rekke større erstatningsposter samt en mindre erstatningspost, som får det utfall at motparten kun får medhold i det som gjelder erstatningsposten av bagatellmessig karakter.*
>
> *Ved vurderingen av om en part har fått medhold i det vesentlige, er det ikke bare forholdet mellom partenes påstander og domsresultatet som er relevant. Det må også ses hen til hvor hovedtyngden i de reelle tvistepunktene har ligget, jf. Rt-2010-727. Det skal således foretas en bredere vurdering enn kun den relative differansen mellom påstand og doms-resultat, se bl.a. Rt-2011-699 og Rt-2013-232. Et avvik fra et angitt maksimumsbeløp kan lettere være forenlig med at saken i det vesentlige er vunnet hvis tvisten hovedsakelig har gjeldt spørsmål om grunnlag for erstatning eller oppreisning, jf. Rt-2010-508.*»

Det er slik retten ser det ikke tvilsomt at Nordlo har fått medhold i det vesentlige, selv om Nordlo ikke fikk medhold i at det forelå en force-majeure hendelse. Det saksøkerne har oppnådd i resultat er av liten og ingen betydning for dem.

Retten har vurdert hvorvidt det foreligger tungtveiende grunner som tilsier at saksøkerne helt eller delvis skal fritas for erstatningsansvar, jf. tvl. §20-2 tredje ledd, men funnet at så ikke er tilfelle.

Nordlo har etter dette krav på full erstatning, som dekker alle deres nødvendige kostnader ved saken, jf. tvl. §20-5 første ledd.

Advokat Skoghøy har lagt frem en omkostningsoppgave på kr. 2 152 570,– for arbeidet han og advokatfullmektig Ohm har gjennomført. Det er ikke fremlagt noen supplerende omkostningsoppgave innen rettens frist den 13.06.2025. Det har ikke kommet innsigelser til omkostningsoppgaven. Omkostningskravet fremstår høyt. Saken gikk over fem rettsdager. Det har vært en rekke provokasjoner underveis i saken. Saken

har reist en rekke tekniske spørsmål og det har vært oppnevnt flere privatoppnevnte sakkyndige i saken for å få saken tilstrekkelig opplyst. Motparten har innhentet både tekniske og økonomiske beregninger som har medført behov for motbevis. Begge parter har rettslige medhjelpere. Det samlede erstatningskravet fra motparten var på over 60 millioner.

Hensett til tvistetemaet og tvistesummen finner retten, selv om beløpet er høyt, under tvil at omkostningene var nødvendige og omkostningsoppgaven legges til grunn. Motparten har selv inngitt en omkostningsoppgave på kr 3 833 483,–

DOMSSLUTNING

1. Nordlo Haugesund AS dømmes til å betale erstatning til Btec AS med 8280-åttetusenfohundreogåtti-kroner innen 14-fjorten- dager fra dommens forkynnelse.
2. Btec As dømmes til å betale erstatning for saksomkostninger til Nordlo med 2 152 570-tomillioneretthundreogfemtitotusenfemhundreogsytti-kroner innen 14-fjorten- dager fra dommens forkynnelse.