



Selmer

Amanda Johnson og Jennifer Parmlind

Ny dom om cybersikkerhet og IT-kontrakter (LG-2025-156056)

Gulating lagmannsrett avsa 30. juni 2026 dom i saken mellom Btec AS («Btec») og Nordlo Haugesund AS («Nordlo»). Btec krevde erstatning etter å ha mistet data da Nordlo, leverandør av ASP-tjenester, ble rammet av et cyberangrep. Saken reiser spørsmål om bindende standardvilkår uten signert kontrakt, grensene for force majeure ved løsepengevirus, og hvor mye som skal til før en IT-leverandørs sikkerhetssvikt er grovt uaktsom. Dommen er anket til Høyesterett og derfor ikke rettskraftig.

I mars 2017 inngikk partene avtale om levering av ASP-tjenester, som innebærer at leverandøren drifter, vedlikeholder og tilgjengeliggjør programvare for kunden via internett. Det ble ikke utarbeidet skriftlig kontrakt. Den 22. april 2021 krypterte trusselaktører store deler av Nordlos driftsmiljø med løsepengeviruset «Ryuk» og krevde 50–60 millioner kroner i bitcoin. Nordlo betalte ikke. Av selskapets 255 kunder mistet fire av dem data helt eller delvis, deriblant Btec. For Btec var konsekvensene store: 14 000 produksjonsmodeller og kritiske ERP-data som ordre- og produktinformasjon, fakturaer og varedokumentasjon gikk tapt. Btec beregnet tapet til 57,2–64,2 millioner kroner. Tingretten tilkjente Btec 8 280 kroner i tråd med ansvarsbegrensningen i Nordlos standardvilkår. Btec anket dommen.

Standardvilkårene var bindende

Lagmannsretten fant at Nordlo hadde rimelig grunn til å forvente at Btec hadde akseptert standardvilkårene, herunder en omfattende ansvarsbegrensning, selv uten signert kontrakt.

Avgjørende var at Btecs bestilling bygget på den samme standardiserte ASP-tjenesten som allerede var etablert for Btecs datterselskap Delta-pump Maskinering AS («DM»). Da daglig leder ba om administratorrettigheter, ble det vist uttrykkelig til DMs ASP-avtale, og samme dag ble tilsvarende tjeneste bestilt for Btec med et ønske om å «samkjøre» virksomhetene. Prisingen ble også knyttet til det DM betalte. Btec må derfor anses for å ha vært kjent med Nordlos standardvilkår.

Vilkårene var heller ikke overraskende eller ubalanserte. Det gjaldt en standardisert tjeneste til 429 kroner per bruker per måned, og tilsvarende ansvarsbegrensninger var utbredt hos sammenlignbare leverandører av ASP- og skytjenester og i statens standardavtaler for IT-anskaffelser. Nordlo tilbød utvidede sikkerhetsløsninger for kunder med særskilte behov, men Btec bestilte ikke dette. En ASP-avtale uten ansvarsbegrensning ville etter rettens syn påført Nordlo en «ikke ubetydelig risiko» ved levering av en standard abonnementstjeneste til beskjedne pris. I tillegg hadde

Nordlo innkalt Btec til oppstartsmøte og forsøkt å komme i kontakt per e-post, uten at Btec møtte eller svarte. At Btec som profesjonell part ikke fulgte opp møteinnkallelser fra Nordlo eller tok skritt for å avklare hvilke vilkår som gjaldt, måtte selskapet selv bære risikoen for.

Standardvilkårenes ansvarsbegrensning utelukket dekning av indirekte tap og begrenset øvrig erstatning oppad til tre måneders leie.

Kontraktsbrudd, men ikke force majeure

Retten konkluderte med at Nordlos utilstrekkelige sikkerhetskopiering og manglende oppetid utgjorde kontraktsbrudd. Deler av Btecs data lå på en RDS-server og den tilhørende backup-serveren som tok sikkerhetskopier var ikke flyttet til det atskilte managementnett slik resten av backup-infrastrukturen var, men lå i samme produksjonsnett (Prodnett 1). Prodnett 1 ble rammet av angrepet og dataene gikk dermed tapt. Sikkerhetskopieringen var utilstrekkelig, og angrepet medførte én virkedags nedetid, slik at kravene til sikkerhetskopiering, drift, tilgjengeliggjøring av programvare og oppetidsgaranti ikke var oppfylt.

Nordlos innsigelse om force majeure førte ikke frem. Løsepengevirus har vært en kjent risiko siden midten av 2010-tallet, og Nasjonal

sikkerhetsmyndighet pekte allerede i 2017 på økt fare for avanserte cyberangrep. Hendelsen var derfor verken ekstraordinær eller upåregnelig for en profesjonell IT-leverandør.

Nordlo har ikke opptrådt grovt uaktsomt

Siste spørsmål var om ansvarsbegrensningen måtte settes til side, slik at Btec kunne kreve full erstatning fordi Nordlo hadde opptrådt grovt uaktsomt.

Retten presiserte at grov uaktsomhet krever et markert og klart klanderverdig avvik fra forsvarlig handlemåte, vurdert ut fra risikoens størrelse, skadesannsynlighet, tilgjengelige forebyggende tiltak, skadepolders kompetanse og eventuell svikt i grunnleggende rutiner. Vurderingen må også skje i lys av hva partene hadde avtalt om ytelse, pris og risikofordeling. Avtalen gjaldt en standardisert ASP-tjeneste uten tilleggsbestilte sikkerhetstjenester, og spørsmålet var om sikkerhetsnivået representerte et kvalifisert avvik fra det som var bestilt og betalt for. Retten så hen til Nasjonal sikkerhetsmyndighets grunnprinsipper for IKT-sikkerhet (basert på ISO 27001), men presiserte at avvik fra anbefalt standard ikke i seg selv er grovt uaktsomt.

Retten påviste flere konkrete svakheter. Nordlo var i gang med å flytte backup-serverne til et eget, adskilt managementnett, men serveren som tok sikkerhetskopier av Btecs data var ennå ikke flyttet og lå fortsatt i det rammede produksjonsnettet. Konsekvensen var at både data og sikkerhetskopier ble kryptert i angrepet. Retten fant at segmenteringsarbeidet ikke var feilprioritert. Videre var Btec nærmest til å opplyse om at tjenesten lagret virksomhetskritiske data. Retten uttalte generelt at en ASP-leverandør ikke har noen alminnelig plikt til å orientere kundene om interne arkitekturvalg eller mellomstadier i en pågående

segmenteringsprosess. Retten påpekte at dette kan stille seg annerledes dersom leverandøren kjenner til at kunden har spesielle data eller risikoforhold.

I tillegg manglet Nordlo skriftlige rutiner og krav om flerfaktoraутentisering. Retten fant det ikke sannsynliggjort at det i 2021 gjaldt noe bransjekrav om flerfaktoraутentisering for tilsvarende tjenester, og skriftlige rutiner ville uansett ikke avverget datatapet.

Retten pekte også på visse svakheter ved sikkerhetsovervåkingen og oppdateringen av applikasjonsprogramvarer, men fant det ikke sannsynliggjort at disse svakhetene forårsaket datatapet eller utgjorde en så kvalifisert svikt at Nordlo kunne anses å ha opptrådt grovt uaktsomt.

I helhetsvurderingen vektla retten at beskyttelse mot et trusselbilde i kontinuerlig utvikling er krevende, at angrepet var utført av en velorganisert og teknologisk kompetent aktør, og at sikkerhetsnivået måtte måles mot bransjepraksis for tilsvarende ASP-tjenester til små og mellomstore virksomheter i 2021. Avgjørende for lagmannsretten var at Nordlo hadde implementert flere sentrale sikkerhetstiltak som sikret at hoveddelen av selskapets infrastruktur og backup-løsninger sto imot angrepet. Btecs egen håndtering fikk også en viss, om enn begrenset, betydning. Etter standardvilkårene var kunden selv ansvarlig for å forsikre verdien av egne data, men Btec hadde ikke tegnet slik forsikring.

Verken enkeltvis eller samlet utgjorde svakhetene et tilstrekkelig kvalifisert avvik til at grov uaktsomhet forelå, og misligholdet av kjerneytelsen var ikke så gjennomgripende at ansvarsbegrensningen kunne settes til side eller tolkes innskrenkende.

Btec ble, som i tingretten, tilkjent 8 280 kroner i erstatning, tilsvarende tre månedsløst. Btec ble også pålagt å betale Nordlos sakskostnader på 2 320 647 kroner.

Hva kan vi lære av dommen?

Dommen etterlater et tydelig budskap. Terskelen for grov uaktsomhet er høy, særlig når et profesjonelt utført cyberangrep rammer en standardtjeneste levert til beskjedent vederlag, uten bestilte tilleggsytelser, fra en lokal leverandør til små og mellomstore virksomheter. Kravene til sikkerhet måles mot hva som var påregnelig for den bestilte tjenesten, ikke mot hva som i ettertid kan påvises som mulige forbedringer.

For kunder er lærdommen å være tydelig overfor leverandøren om hvilke data som er virksomhetskritiske, og å forstå at ansvaret for å bestille eller presisere sikkerhetsbehov ligger hos kunden selv. Aller helst bør avtalen si uttrykkelig hvilket sikkerhetsnivå som forventes, men da må kunden også være forberedt på å betale for det. Kunder som forholder seg passive, bærer også risikoen for dette.

For leverandører er det viktig merke seg at en generell force majeure-bestemmelse ikke er et forsvar mot cyberangrep. Løsepengevirus, som var tema i denne saken, anses som en kjent og påregnelig risiko for en profesjonell IT-leverandør.

Avslutningsvis er aktsomhetsnormen dynamisk. Retten bedømte Nordlo etter bransjepraksis i 2021, og fremhevet blant annet at Microsoft først innførte krav om multifaktoraутentisering for eksisterende kunder i januar 2025. Det som var forsvarlig den gang, er ikke nødvendigvis forsvarlig nå, verken for leverandører som vurderer eget sikkerhetsnivå eller for kunder som vurderer et krav.

Amanda Johnson, advokatfullmektig og Jennifer Parmlind, senioradvokat. Begge arbeider særlig med teknologi og immaterielle rettigheter i Advokatfirmaet Selmer.

Les dommen her:

<https://lovdata.no/dokument/LGSIV/avgjorelse/lg-2025-156056?q=LG-2025-156056>