Infodesk AS

Rådhusgata 15,

3211 Sandefjord

Regresskravet sendes kun elektronisk til hakon@infodesk.no

Dato: 17.06.2025 Vår ref.: 4314519 Deres ref.:

Krav om tilbakebetaling av utlegg etter cyberangrep hos IDT Solutions AS

Det vises til fremsatt regressvarsel og senere dialog i saken. Det rettes herved et regresskrav mot Infodesk AS for utlegg etter cyberskade som har oppstått etter cyberangrep på nettsiden til IDT Solutions AS den 03.04.2023. Infodesk AS mottar regresskravet som underleverandør av nettsideløsningen til IDT Solutions.

Crawford & Company (Norway) AS er et selvstendig oppgjørsselskap, som i denne forbindelse behandler cyberskaden under IDT Solutions sin forsikring hos Fremtind Forsikring AS (heretter forsikringsgiver). Crawford & Company representer Fremtind Forsikring i saken, og fremmer regresskravet på vegne av dem.

1. SAKENS FAKTISKE SIDE

IDT Solutions (heretter skadelidte) ble utsatt satt for et cyberangrep den 02.04.2023, hvor hackerne hadde tilgang til nettsiden og gjorde uautoriserte endringer senest 12.04.2023. Skadelidte har to nettsider som hovedleverandør drifter, idt.no og idtsports.com. Infodesk AS (heretter Infodesk AS eller skadevolder) er underleverandør og bistår hovedleverandør i leveringen av nettløsningen. Det var idtsports.com (heretter nettsiden) som ble utsatt for cyberangrep og skadet. IDT ble oppmerksom på angrepet den 05.03.2023 da kunder tok kontakt siden betalingsløsningen til nettsiden ikke fungerte.

IDT Solutions inngikk to separate, løpende kontrakter med hovedleverandør Ess Design i februar 2021 om levering av løsningen for begge deres nettsider, herunder drift, vedlikehold og videreutvikling av nettsideløsningen. Fra avtalen mellom partene hitsettes det:

> "*Driftsavtale og sikkerhetsoppdateringer: Regelmessig sikkerhetsoppdatering av publiserings-løsningen er nødvendig slik at nettstedet til enhver tid er oppdatert med det nyeste av programvare og beskyttelse mot uvedkommende. Vi oppdaterer jevnlig programvare og overvåker hjemmesiden for å raskt oppdage eventuelle problemer. Dette utføres av ess Design til en månedlig pris, kr 750,- eks. Mva.*"

Her fremkommer det at ESS Design og Infodesk AS som underleverandør sitt ansvar innebærer å utføre nødvendige oppdatering som sørger for at nettsiden er best mulig beskyttet mot cyberangrep i henhold til nyeste tilgjengelige oppdateringer.

Skadelidte og hovedleverandør var i perioden for cyberangrepet i en konflikt om fakturaer knyttet til idt.no. Dette førte til at hovedleverandør sluttet å drifte, vedlikeholde og oppdatere begge nettsidene til skadelidte. Dette innebar at leverandørene også nektet å oppdatere nettsiden (idtsports.com) som ble påført cyberangrepet, som ikke var innblandet i konflikten. Denne nettsiden hadde en kontrakt som var uavhengig av den andre nettsiden, og ved å nekte å oppdatere nettsiden brøt skadevolder kontrakten mellom partene.

På grunn av konflikten holdt skadelidte på å endre leverandør av nettsiden fra Ess Design med underleverandører til Kloner den 11.04.2023. Dette førte til at den nye leverandøren Kloner bisto med å slå ned angrepet og opprydning av skadene.

Truesec som er et eksternt konsulentfirma som jobber med it-sikkerhet, ble den 12.04.2023 engasjert av Crawford til å bistå med å håndtere hackerangrepet og drive forensics for å finne ut hvordan hackerangrepet fant sted. Skadelidte meldte hackerangrepet til Datatilsynet den 13.04.2023, da nettsiden inneholder personopplysninger om kunder. For å få en sikker nettside til å fungere så raskt som mulig igjen, byttet skadelidte til en annen plattform for nettsiden.

Skadevolderne anfører at det var den nye tilbyderen av nettsiden som sto bak hackerangrepet, i et forsøk på å få kontrakten fra skadelidte. Dette bestrides av skadelidte og er ikke forenelig med funnene i skaderapporten som er utarbeidet av Truesec og svakhetene ved programvaren som ble allmennkjent i ettertid.

Truesec sin rapport etter hendelsen konkluderer med årsaken til cyberangrepet. I rapporten fremkommer det at hackerne utnyttet en svakhet hos nettbutikker som er utviklet og driftet med WooCommerce gjennom Wordpress. Wordpress er en leverandør som tilbyr software for å utvikle og drifte nettsider, mens WooCommerce er en plugin hos Wordpress som kan brukes til å utvikle og drifte nettbutikker. Det var en annen plugin til Wordpress som brukes til å utvikle nettsider, Elementor Pro, som inneholdt en svakhet som hackere kunne utnytte til å få kontroll på nettsider.

Svakheten ble kjent for utviklerne av Elementor Pro den 18.03.2023, og allmennkjent etter at en it-blogg (Nintechnet) publiserte en artikkel som redegjorde for svakheten og hvordan den kan utnyttes den 28.03.2023. Det ble da kjent at nettsider som brukte versjon 3.11.6 eller eldre av pluginen, inneholdt svakheten. Det ble også kjent at oppdateringen til 3.11.7 versjonen som ble tilgjengelige den 22.03.2023, ikke innholdet svakheten lengre. Nettsider som var oppdatert til denne versjonen kunne ikke bli hacket gjennom den kjente svakheten.

Dersom nettsiden til skadelidte var oppdatert til den nyeste oppdateringen 3.11.7, ville svakheten vært utbedret og nettsiden vært sikret mot cyberangrepet og påfølgende skader. Oppdateringen var tilgjengelig 11 dager forut for cyberangrepet.

2. SAKENS RETTSLIGE SIDE

Skadeerstatningsloven § 4-3 stadfester at skadelidtes forsikringsgiver kan kreve regress for tingskader eller annen formueskade fra den ansvarlig skadevolder for utbetalt erstatning. Forsikringsgiver kan kreve regress etter bestemmelsen så langt den skadelidte kunne ha krevd erstatning hos skadevolder etter § 4-2.

Infodesk AS forårsaket skaden i utførelsen av sitt yrke. Infodesk AS var kontraktsfestet som underleverandør til å drifte, vedlikeholde og videreutvikle nettsiden, og hadde et formål om å oppnå fortjeneste. **Skadeerstatningsloven § 4-3, jf. § 4-2 bokstav b åpner dermed for å kreve regress fra skadevolder.**

Videre så stadfestes det i rettspraksis at hjemmelen for regress kan være *lov, avtale og alminnelige* rettssetninger, jf. HR-2017-2414-A. I denne saken så foreligger det en kontrakt/avtale mellom partene, som åpner for at skadelidte kan kreve regress fra skadevolder som er skyld i skaden.

At en skadevolder har opptrådt uaktsomt vil si at vedkommende har handlet i strid med handlingsnormen som foreligger i den gitte situasjonen.

I denne saken har Infodesk AS og hovedleverandør ved å bevisst nekte å oppdatere programvaren til nettsiden opptrådt erstatningsbetingende uaktsomt og er skyld i skaden. Skadevolder hadde eller burde hatt kunnskap om at unnlatelsen åpnet for mulige cyberangrep og skader hos skadelidte. Infodesk AS var kontraktsfestet til å drifte, vedlikehold og oppdatere nettsiden. Ved å nekte å oppdatere nettsiden brøt skadevolder kontrakten mellom partene.

Det foreligger også et konkret formuestap for skadelidte, som har direkte sammenheng med skadevolders unnlatelse. Det er også tilstrekkelig årsakssammenheng mellom skadevolders unnlatelse og inntruffet skade som følge av cyberangrepet. Den nye oppdateringen som var tilgjengelig inneholdt ikke svakheten som åpnet for hackerangrepene. Hvis skadevolder hadde oppdatert nettsiden i henhold til sitt ansvar, ville ikke skaden ha inntruffet.

3. FREMTINDS KOSTNADER

Fremtind har foretatt en forsikringsutbetalinger basert på de kostnadene som er oppstått i saken. Følgende kostnader er dekket av Fremtind:

Dato	Leverandør	Valuta	NOK	Kommentar
21.04.2023	SYSE AS		498,40	Eksportere logger
30.04.2023	Lindbak IT AS		1 050,00	Møte 13.04.23 i forbindelse med angrepet
30.04.2023	ECI Software Solutions Norway AS		3 100,00	Set up of Spectra etter angrepet
30.04.2023	Truesec Group AB	313 600 SEK	305 484,00	Incident response og forensic
30.05.2023	SYSE AS		627,00	Linux webserver transfer 20.07.23 - 20.10.23
08.05.2023	Kloner AS		74 700,00	Response hack, cleanup. Set up av ny webside, Kjøp av modules
31.05.2023	Truesec Group AB	7 350 SEK	7 154,77	Incident Report
06.06.2023	Kloner AS		37 900,00	arbeid på website
Sum kostnader			**430 514,17**	

- Valutarate ved utbetaling 1 SEK =1,02 NOK

IDT solutions AS har en egenandel på kr. 10.000 som er inkludert i kravet på kr. 430.514.

Det er utover overnevnte krav meldt av sikrede at de har blitt påført eget driftstap. Dette er ikke blitt dekket av Fremtind.

4. KRAV

På bakgrunn av dokumentasjonen og opplysningene i saken er Ess Design erstatningsbetingende ansvarlig for skadene som har oppstått etter cyberangrepet hos skadelidte. Derfor holdes Infodesk AS solidarisk ansvarlig sammen med hovedleverandør for kravet på NOK 430.514.

Kraves bes innbetalt til vår klientkonto 6003.05.23108 innen 14 dager. Vennligst bemerk betalingen med vårt saksnummer «4314519».

Vi imøteser deres betaling.

Med vennlig hilsen

Øystein Gunleiksrud

Crawford & Company