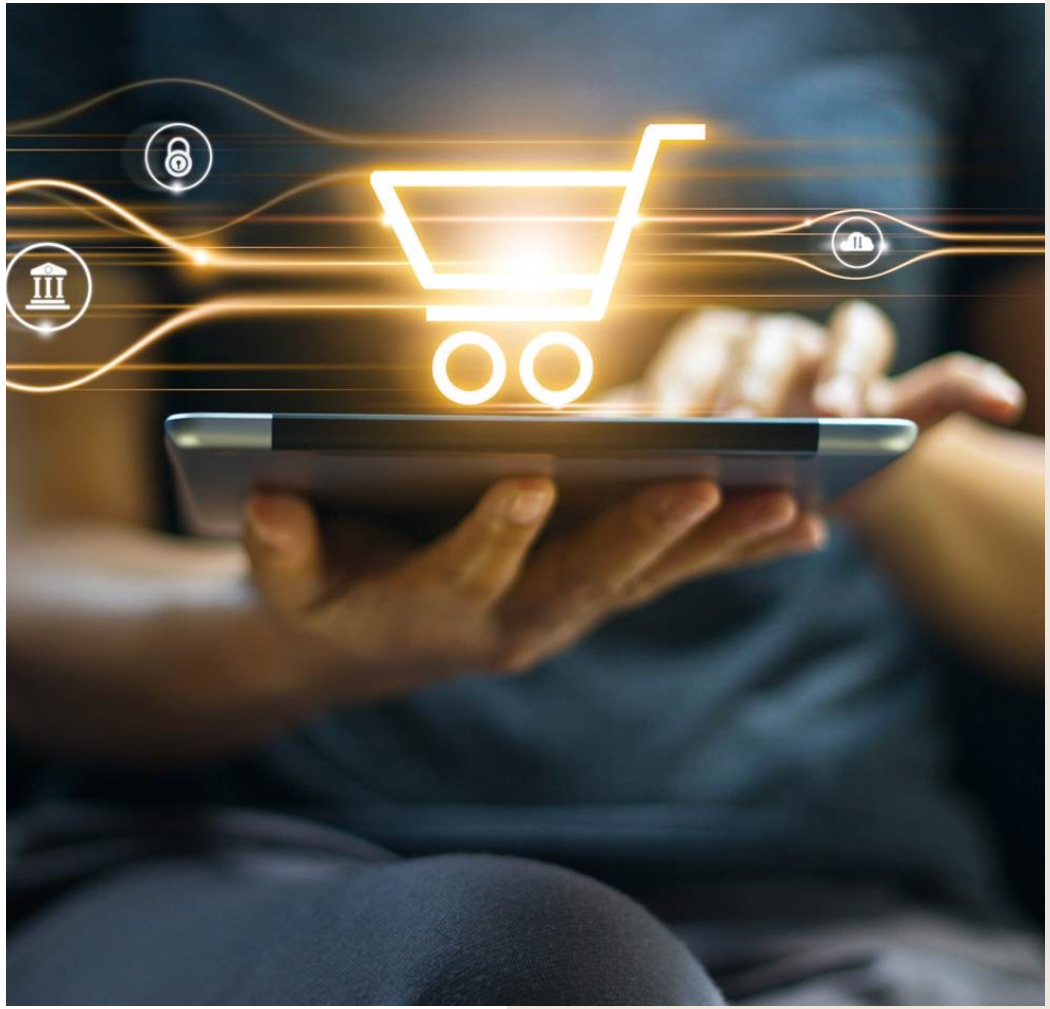
ENERGIBRANSJENS INNKJØP- OG KONTRAKTSKONFERANSE 1. JUNI 2023

Cyberberedskap – rettslige aspekter

CHRISTOPHER CLAUSEN

THOMMESSEN

Godt cyberberedskap fra et rettslig perspektiv handler om kunnskap om trusselbildet, gode risikoanalyser og kontroll på rettslige forpliktelser, proaktivt og reaktivt.



Introduksjon

- Økt grad av digital tilstedeværelse og angrepsflater innebærer økt eksponering
- PST og NSM: Stadig økende aktivitet og mer komplisert trusselbilde
- Statlige og private aktører
- Motivasjon for å angripe:
  - Bryte ned selskapers forretningsaktiviteter; og
  - Bryte ned kritisk infrastruktur.
  - Kan være økonomisk og/eller politisk motivert
- Ingen cybersikkerhetslov – fragmentert lovgivning

Typer angrep:

Denial of Service (DOS) – angrepet resulterer effektivt i utilgjengelige systemer/tjenester

Malware – virus som setter enheten i ustand

Phishing – tilsynelatende legitime forespørsler som "fisker" etter informasjon eller aktivitet

Rettslige konsekvenser av et cyberangrep

Bøter og sanksjoner

Tap av IP og data

Erstatningskrav

Bistand fra tredjeparter

Massesøksmål

Notifikasjonskrav (+ kostnader)

Styreansvar

Brudd på straffelov

Tap av kontrakter

Tap av renomme

Regulatoriske/lovfestede forhold

- Ingen generell lov som regulerer cybersikkerhet og cyberberedskap – fragmentert regelverk
- Generelle regulatoriske krav:
  - GDPR (se f.eks. artikkel 32 om sikkerhet ved behandlingen)
  - Sikkerhetsloven
  - Selskapsrett (styreansvar mv.)
- Sektorspesifikke regler
  - Energisektoren – kraftberedskapsforskriften
  - Bank- og finanssektoren – IKT-forskriften
  - Helsesektoren – pasientjournalloven m.fl.
- Kommende lover:
  - **Network and Information Security Directive (NIS II)**
  - Digital Operational Resilience Act (DORA)

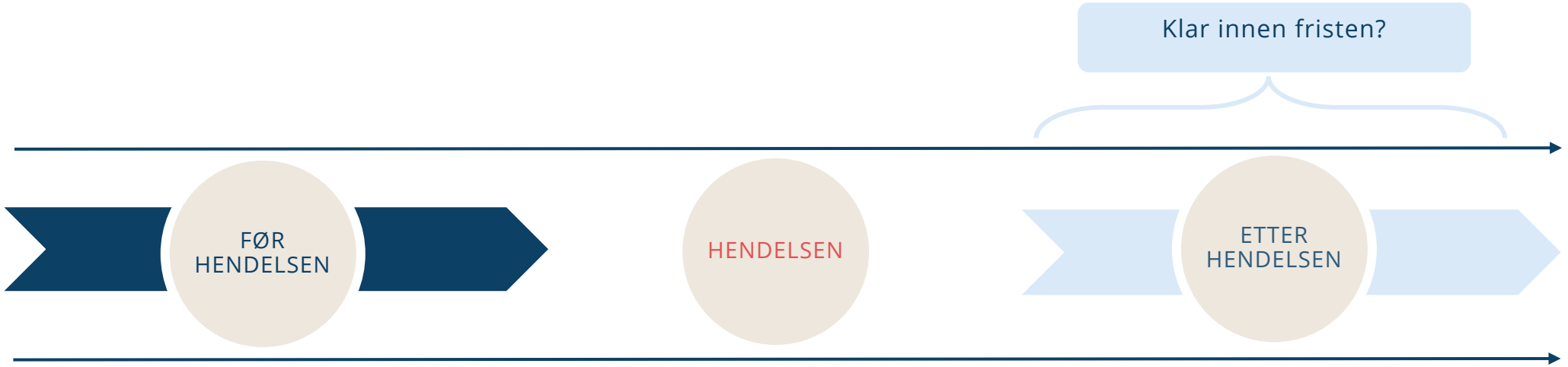
Kontraktsrettslige aspekter

- Posisjonen i verdikjeden vil avgjøre omfanget av rettslig eksponering i en cyberkontekst
- Oversikt og kontroll på rettigheter og forpliktelser bidrar til å sikre god responsevne og håndtering av det juridiske etterspillet ved et angrep
    - Kontroll på verdikjeden og sentrale kontrakter med kunder og leverandører /samarbeidspartnere
    - IT-kontrakter
    - Samarbeidsavtaler/JVs mv

Relevante kontraktsbestemmelser

- Forpliktelser som sikrer regulatorisk etterlevelse
  - Overholdelse av krav om forsvarlig sikkerhet, varslingsplikter mv.
  - Konsekvensene av partenes manglende oppfyllelse av slike krav
- Ansvarsbegrensninger og skadesløsholdelse
- Varslingsplikter
- Særskilte krav til cybersikkerhet og -beredskap?
- Back-up av kundedata
- Konfidensialitetsforpliktelser – forretningshemmeligheter og sensitive data
- Hvordan kan avtalen utformes på måte som sikrer effektiv samhandling med berørte kunder, leverandører og samarbeidspartnere
- Back-to-back: Sikre at regulatoriske og kontraktuelle forpliktelser er videreført til bakenforliggende ledd i verdikjeden

Håndtering av cyber-/ransomangrep



Kjenn dataene dine og eksponeringen	Sette i gang rutiner for håndtering av hendelser	Krav om varsling
Kontraktspraksis	Engasjere eksperter og forsikringsselskap	Kartlegging
Tilstrekkelige tekniske og organisatoriske tiltak	Å betale eller ikke betale…?	Bevis
		Involvere politi?
		Tette avvik

Thommessen CyberHub

Your one-stop-shop for cyberassurance services

Our own legal specialists have teamed up with international experts on attack emulation, cyber security, insurance and data protection to form a new service platform for cyberassurance.

Our cross-functional team has developed a number of integrated services and smart solutions to support you on all aspects of cyber risk assurance and help you reduce your digital exposure.

Understand

Understand the threat landscape and your vulnerabilities

Prepare

Reduce the technical and legal exposure of your data

Respond

Get 24/7 response support with cyber related incidents

Takk for oppmerksomheten

thommessen.no
Oslo • Bergen • Stavanger • London

Christopher
Sparre-Enger Clausen
PARTNER // ADVOKAT

Oslo
M +47 93 05 38 54
E csc@thommessen.no