RAPPORT

# Risikostyring i digitale verdikjeder

Rapport fra en arbeidsgruppe ledet av professor Olav Lysne

dsb
Direktoratet for samfunnssikkerhet og beredskap

Utgitt av: Direktoratet for samfunnssikkerhet og beredskap (DSB) 2020

ISBN: ISBN 978-82-7768-496-3 (PDF)

Grafisk produksjon: ETN Grafisk, Skien

# Risikostyring i digitale verdikjeder

Rapport fra en arbeidsgruppe ledet av professor Olav Lysne

# SAMMENDRAG


Gjennom de første to tiårene av 2000-tallet har det vært en rask utvikling, hvor mange av de verdikjedene samfunnet er avhengig av har endret karakter til i større eller mindre grad å bli basert på direkte kobling mellom datamaskiner. Endringene har medført at nye sårbarheter har oppstått. De digitale verdikjedene er komplekse, lite oversiktlige, tett koplete og i stor grad transnasjonale. En feil et sted i kjeden kan medføre momentan svikt i viktige tjenesteleveranser et helt annet sted.

Justis- og beredskapsdepartementet ga høsten 2018 Direktoratet for samfunnssikkerhet og beredskap (DSB) i oppdrag å nedsette en arbeidsgruppe som skulle foreslå et nasjonalt rammeverk for at myndighetene skal kunne ha en samlet oversikt over digitale verdikjeder, og en modell for at virksomhetene selv kan etablere oversikt over slike kjeder. Oppdraget er en oppfølging av NOU 2015:13 *Digital sårbarhet – sikkert samfunn*.

Arbeidsgruppen, som har vært ledet av professor Olav Lysne, har vektlagt å utarbeide en modell for risikostyring i digitale verdikjeder primært innrettet mot den enkelte offentlige eller private virksomhet. Modellen vil også kunne understøtte nasjonal risikostyring (governance).

I rapporten drøftes ulike risiko- og sårbarhetsforhold knyttet til digitale verdikjeder nærmere. Her inngår blant annet falsk eller svekket redundans, dvs. at redundante løsninger deler sårbarheter lenger ned i verdikjeden, ulike former for avhengighet og forhold knyttet til verdikjedenes transnasjonale karakter.

Modellen arbeidsgruppen har utarbeidet skal for det første tjene som veiledning i hvordan en virksomhets interne risiko- og sårbarhetsvurdering kan fange inn sårbarheter som propagerer gjennom komplekse digitale verdikjeder. For det andre skisserer rapporten hvordan en virksomhet kan fremskaffe informasjon om sine leverandørers verdikjeder. For det tredje skal modellen være til hjelp for en virksomhet som har behov for oversikt over hvilke digitale verdier den bidrar til, og dermed har delansvar for.

Modellen er strukturert på basis av NS-ISO 31000:2018 *Risikostyring. Retningslinjer* med følgende fem trinn:

*1. Omfang og kontekst – behov for oversikt over digitale verdikjeder*

- Er det nødvendig å få oversikt over den digitale verdikjeden som virksomhetens leverandører er avhengig av?
- Hvilke interne og eksterne kontekstuelle forhold bør tas med i betraktning når videre vurderinger skal gjøres?

2. *Risikoidentifisering – informasjonsinnhenting*

- Dersom svaret på det første spørsmålet over er «ja», fra hvilke leverandører bør virksomheten innhente denne oversikten?
- Hvor langt ned i kjeden er det ønskelig og mulig å skaffe oversikt, og hvilke opplysninger bør leverandørene bes om å fremskaffe?

3. *Risikoanalyse*

- På bakgrunn av de innhentede opplysningene, hvordan vurderer virksomheten risiko knyttet til hendelser i verdikjeden?
  - Hvor sannsynlig er slike hendelser?
  - Hvilke konsekvenser kan de få?
  - Hvor sikre er man på disse vurderingene?

*4. Risikoevaluering og risikohåndtering*

- I hvor stor grad er virksomheten villig til å akseptere den risikoen som er avdekket?
- Hvor stort er potensialet for risikoreduksjon?
- Hvilke tiltak kan redusere risikoen til et (mer) akseptabelt nivå?
- Er disse tiltakene forsvarlige ut fra en nytte/kostnadsvurdering og positive og negative bieffekter av tiltaket?

*5. Implementering av tiltak*

- Hvordan skal tiltak implementeres og følges opp?

For hvert av trinnene er det definert underspørsmål som skal være til hjelp i virksomhetens arbeid med å kartlegge verdikjedene og håndtere den risikoen som avdekkes.

Rapporten omtaler videre risikostyring av digitale verdikjeder på samfunnsnivå. Myndighetenes interesse på dette området er primært knyttet til sikkerheten i digitale verdikjeder som har stor betydning for befolkningen og samfunnet. Virkemidler staten rår over er imidlertid ikke tilstrekkelige for å kunne styre sikkerheten i digitale verdikjeder av kritisk betydning for samfunnet fullt ut.

Derfor må ulike typer virkemidler brukes i kombinasjon for å påvirke sikkerheten på best mulig måte. Disse tiltakene omtales som harde og myke governance-tiltak, der reguleringer av ulike slag er viktigst blant de harde tiltakene. I rapporten fremheves også de mykere tiltakene som for eksempel utarbeidelse og implementering av internasjonale standarder. Det er naturlig å se slike tiltak i sammenheng med «Internasjonal cyberstrategi for Norge» (UD 2017).

Modellen for risikostyring i digitale verdikjeder i virksomheter vil være et sentralt virkemiddel også for myndighetene. Modellen kan knyttes opp mot hard governance i form av reguleringer. I tillegg kan modellen være et mykt tiltak gjennom å innarbeides som beste praksis.

Arbeidsgruppen har følgende anbefalinger:

- *Problemstillinger og utfordringer knyttet til sikkerhet i digitale verdikjeder bør utdypes i NSMs grunnprinsipper for IKT-sikkerhet.*
- *NSM bør utgi anbefaling for risikostyring i digitale verdikjeder som en operasjonalisering av NSMs grunnprinsipper for IKT-sikkerhet. Utgangspunktet er modellen som presenteres i kapittel 4 i denne rapporten.*
- *NSM bør videreutvikle den anbefalte modellen for risikostyring av digitale verdikjeder sammen med relevante aktører og i lys av lignende arbeid som foregår internasjonalt.*
- *Modellen for risikostyring i digitale verdikjeder bør tas inn i, eller refereres til, i NSMs veiledere til sikkerhetsloven med forskrifter.*
- *Ved en fremtidig evaluering av sikkerhetsloven med forskrifter bør det legges særlig vekt på å vurdere i hvilken grad loven har bidratt til å styrke sikkerhet i digitale verdikjeder.*
- *Ved revisjon av loven og dens forskrifter bør det vurderes å tydeliggjøre at virksomheter som er underlagt loven selv skal ha oversikt over egne digitale verdikjeder av betydning for grunnleggende nasjonale funksjoner, og at denne oversikten skal gjøres tilgjengelig for sikkerhetsmyndigheten.*
- *En påpekning av viktigheten av å kartlegge og redusere sårbarheter i digitale verdikjeder bør tas inn i forskriften til ny lov om sikkerhet i nettverk og informasjonssystemer (NIS-direktivet i norsk lov). I veiledning til loven bør det vises til NSMs grunnprinsipper og modell for risikostyring i digitale verdikjeder.*
- *Tilsvarende bør modellen for risikostyring i digitale verdikjeder tas inn i forskrifter og veiledere til relevant sektorlovverk.*
- *Ved revisjon av KIKS-rammeverket bør det pekes på hvordan departementene (og andre myndighetsaktører) kan arbeide for å kartlegge og redusere sårbarheter. I denne sammenheng bør sårbarheter i digitale verdikjeder omtales spesielt, og det bør henvises til modell for risikostyring i digitale verdikjeder.*
- *Justis- og beredskapsdepartementet bør utrede nærmere og beslutte hvordan ulike statlige virkemidler skal benyttes for en overordnet samfunnsmessig risikostyring av digitale verdikjeder av stor betydning for befolkningens og samfunnets sikkerhet. Elementer i denne sammenheng kan være:*

  - *Veiledning for å fastsette digitale verdier*
  - *Veiledning for nivåspesifisering av akseptert digital sårbarhet*
  - *Sårbarhets- og verdivurderinger ved større avtaleinngåelser*
  - Forsknings- og utviklingstiltak

- Justis- og beredskapsdepartementet, Forsvarsdepartementet, Utenriksdepartementet og øvrige aktuelle sektordepartement bør se til at Norge tar del i internasjonale initiativer for å etablere standarder, samt identifisere og implementere tiltak utviklet internasjonalt som gir mer effektive og sikre digitale verdikjeder.
- Regjeringen bør vurdere å utarbeide en strategi for ivaretagelse av sikkerhet i transnasjonale digitale verdikjeder

KAPITTEL

# 01

# Innledning

Gjennom 70- og 80-tallet var de aller fleste datamaskiner isolerte enheter. Det arbeidet de utførte inngikk i verdikjeder, men maskinene kommuniserte ikke direkte med andre maskiner i andre virksomheter. Alt samarbeid mellom virksomheter foregikk analogt og mellom mennesker.

Kommersialiseringen av internett gjennom 90-tallet endret denne situasjonen. To datamaskiner i to forskjellige virksomheter kunne da gjennom internett kommunisere direkte med hverandre og samarbeide uten at mennesker var involvert.

Gjennom de første to tiårene av 2000-tallet har det vært en rask utvikling hvor mange av de verdikjedene vi som samfunn er avhengige av, har endret karakter til i større eller mindre grad å være basert på direkte kobling mellom datamaskiner. Dette gjelder blant annet kraftforsyning, helsetjenester, vannforsyning til befolkningssentra, trafikk på vei, bane, sjø og i luften, kommunikasjonstjenester, finansielle tjenester og industriell produksjon.

Endringene har medført at mange viktige prosesser og tjenester er blitt betydelig mer effektive. Samtidig har de medført nye sårbarheter. De digitale verdikjedene er komplekse, lite oversiktlige, tett koplete og transnasjonale. En feil et sted i kjeden kan medføre momentan svikt i viktige tjenesteleveranser et helt annet sted.

# 1.1 MANDAT

Arbeidsgruppens oppdrag er formulert i oppdragsbrev fra Justis- og beredskapsdepartementet (JD) til DSB datert 11. oktober 2018:

> «Lysneutvalget foreslår i NOU 2015:13 "Digital sårbarhet – sikkert samfunn" å etablere et nasjonalt rammeverk for å ivareta en helhetsvurdering av digitale verdikjeder. Utvalget begrunner dette bl.a. ved at lange og uoversiktlige verdikjeder som spenner over flere sektorer, nivåer og landegrenser, er en kjerneutfordring ved vurdering av digital sårbarhet. Videre fremheves det at komplekse digitale verdikjeder er et vesentlig hinder for å kunne fastslå hvilken digital sårbarhet vi har, og at dette finner Lysneutvalget igjen i alle sektorer som de omhandler i rapporten. For en utdyping av forslag til tiltak og bakgrunn for anbefalingen se tiltak 23.1 i rapporten.
>
> *Beskrivelse av oppdraget*
>
> Som en oppfølging av Lysneutvalgets anbefaling ønsker vi at Direktoratet for samfunnssikkerhet og beredskap (DSB) nedsetter en arbeidsgruppe, med bl.a. ressurser fra DSB, for å foreslå et nasjonalt rammeverk for å ivareta en helhetsvurdering av digitale verdikjeder. I dette inngår det både å foreslå et nasjonalt rammeverk for at myndighetene skal kunne ha en samlet oversikt, og en modell for at virksomhetene selv kan etablere oversikt over sine digitale verdikjeder. […]»

## 1.1.1 ARBEIDSGRUPPENS MANDATFORSTÅELSE

Arbeidsgruppen har vektlagt å utarbeide en modell for risikostyring i digitale verdikjeder primært som et hjelpemiddel for offentlige og private virksomheter. Modellen er generisk og skal kunne benyttes på tvers av samfunnssektorer og virksomhetstyper. En slik modell vil være et verktøy for å styre risikoen i virksomhetens verdikjeder.

Modellen skal legge til rette for operasjonalisering av arbeid med å identifisere sårbarheter i digitale verdikjeder på virksomhetsnivå ved å:

- støtte virksomheter i arbeidet med å etablere oversikt over hvilke verdier deres kunder kan gjøre dem ansvarlig for
- støtte virksomheter i arbeidet med å få oversikt over hvordan de arver sårbarheter fra sine leverandørkjeder, og hvordan den risikoen dette representerer kan håndteres

Modellen vil i tillegg kunne understøtte nasjonal risikostyring ved å:

- bidra til å identifisere informasjonssystemer som er av avgjørende betydning for grunnleggende nasjonale funksjoner (GNF) i henhold til

sikkerhetsloven, samt avhengigheter i den forbindelse
- støtte arbeidet med sikkerhet i digitale verdikjeder med basis i sektorlovverket
- støtte arbeidet med å gjennomføre risikovurdering av nettverk og informasjonssystemer som benyttes for å levere en digital tjeneste i henhold til NIS-direktivet
- danne grunnlag for fremtidige regulatoriske risiko- og sårbarhetsvurderinger hvor digitale verdikjeder inngår som en sentral komponent

Modellen er i seg selv ikke tilstrekkelig til å gi myndighetene oversikt over og evne til å styre risikoen på samfunnsnivå. Dette krever også andre virkemidler. Arbeidsgruppen skisserer i kapittel 5 hvordan modellen kan inngå i en større sammenheng.

Rapporten er skrevet for Justis- og beredskapsdepartementet, og arbeidsgruppens anbefalinger har derfor primært et myndighetsperspektiv. Arbeidsgruppens mandatsforståelse er avklart med departementet.

# 1.2 BEGREPSBRUK

### 1.2.1 RISIKOSTYRING OG GOVERNANCE

Begrepet risikostyring brukes i rapporten slik det er definert i standarden NS-ISO 31000:2018 Risikostyring – retningslinjer: "Koordinerte aktiviteter for å rettlede og kontrollere en organisasjon med hensyn til risiko."

Risikostyringsprosessen dreier seg på den ene siden om å få innsikt i risikoforhold, effekt av tiltak og grad av styrbarhet av risiko. På den andre siden handler den om metoder, prosesser og strategier for å kunne kartlegge og styre risikoforholdene.[1]

[1] Aven, Røed og Wiencke (2008).

Risikostyring skjer både på samfunnsnivå og på virksomhetsnivå. På samfunnsnivå er dette i hovedsak en myndighetsoppgave. Virkemidlene myndighetene rår over er annerledes enn de den enkelte virksomhet kan benytte seg av. I rapporten benyttes derfor også begrepet "governance" om risikostyring på samfunnsnivå. "Governance" forstås her som overordnede prosesser og strategisk/politiske virkemidler som utøves av myndighetene på tvers av virksomheter og sektorer for å sikre at drift og utvikling av digitale verdikjeder foregår i tråd med nasjonale strategier og politisk intensjon og politiske målsettinger. Dette kan innbefatte arbeid på internasjonale arenaer.

Risiko i digitale verdikjeder omfatter risiko knyttet til tap av konfidensialitet og/eller integritet i, og/eller tilgjengeligheten av, informasjon eller informasjonssystemer som medfører konsekvenser for egen organisasjon, andre organisasjoner, enkeltpersoner og/eller samfunnet. Risikostyring i digitale verdikjeder beskriver prosesser knyttet til å identifisere, vurdere og begrense risikoen knyttet til slike kjeder.

### 1.2.2 GRUNNLEGGENDE TEKNISKE DEFINISJONER

Hardware er et berørbart, fysisk digitalt produkt. Eksempler på hardware er en fiberkabel, et kretskort, en chip, en mobiltelefon eller en PC.

Software er en logisk og som oftest tekstlig beskrivelse av hvilke handlinger hardware skal utføre. Eksempler på software er et operativsystem, en driver eller en applikasjon (app).

En digital tjeneste er en gjentagende virksomhetsaktivitet med et definert resultat og utføres av digitalt utstyr bestående av hardware og software.

En digital infrastruktur består av hardware og software og utfører en eller flere tjenester. Mobiltelefonnettet er et eksempel på en infrastruktur som leverer telefoni, meldingstjenester og internett-tilkobling.

En digital infrastruktur kan bestå av flere deler som er eiet, vedlikeholdt og drevet av forskjellige organisasjoner. Hver av disse delene leverer da

digitale tjenester til de andre delene i infrastrukturen, slik at den samlet sett leverer de tjenestene den skal. Sluttjenesten til infrastrukturen – som for eksempel telefoni – er altså avhengig av at de forskjellige delene hver for seg leverer definerte digitale tjenester til hverandre.

### 1.2.3 DEFINISJON AV DIGITAL VERDIKJEDE

En digital verdikjede er en struktur av leveranser mellom virksomheter, hvor hver leveranse enten er en digital tjeneste, software eller hardware.[2]

En oversikt over en digital verdikjede består derfor i en oversikt over en fysisk infrastruktur, samt hvem som eier, vedlikeholder og opererer de forskjellige delene av denne. Videre vil den bestå av en oversikt over hvilke digitale tjenester som utveksles mellom de forskjellige delene, samt hvilken hardware og software som inngår.

Rapporten retter i første rekke oppmerksomheten mot digitale tjenester som leveres mellom virksomheter i en digital infrastruktur. Leveranser av hardware og software til infrastrukturen kan i noen grad fanges inn av arbeidsgruppens modell, men å etablere en fullstendig og detaljert oversikt over historien og leveransekjeden bak alle hardware- og softwarekomponenter er ikke praktisk mulig.

### 1.2.4 LEVERANDØR/UNDERLEVERANDØR

I beskrivelsen av aktørene i verdikjedene brukes betegnelsene virksomhet, leverandør, underleverandør og kunde.

Alle aktører i verdikjedene er *virksomheter*, også myndighetsorganer selv om disse også har en annen rolle. Virksomhetene gjør avtaler om leveranser fra andre virksomheter som da er å regne som deres *leverandører*. Disse kan igjen ha sine egne leverandører som da er *underleverandører* til de førstnevnte virksomhetene.

En *kunde* er i denne sammenheng en kjøper av en digital tjeneste.

## 1.3 GRUPPENS SAMMENSETNING OG ARBEID

Arbeidsgruppen har bestått av:

- professor Olav Lysne, Universitetet i Oslo (leder)
- spesialrådgiver Tor Saglie, Justis- og beredskapsdepartementet
- utredningsleder Harald Fardal, Direktoratet for samfunnssikkerhet og beredskap
- seniorrådgiver Line Ugland Nyseth, Nasjonal kommunikasjonsmyndighet
- seniorrådgiver Berit Salvesen, Nasjonal sikkerhetsmyndighet
- seniorrådgiver Ernst Unsgaard, Nasjonal sikkerhetsmyndighet

Arbeidsgruppen har hatt åtte møter fra januar til september 2019 og har vært støttet av et sekretariat bestående av fagdirektør Erik Thomassen og utredningsleder Janniche Cramer fra Direktoratet for samfunnssikkerhet og beredskap og seniorrådgiver Roger Kolbotn fra Justis- og beredskapsdepartementet.

Arbeidsgruppen har fått informasjon fra enkelte virksomheter underveis i prosessen. Oversikt over samtaler, øvrig dokumentasjon og kilder som er benyttet i arbeidet, fremkommer i vedlegget til rapporten.

[2] Begrepet digital verdikjede brukes gjennomgående i NOU 2015:13 *Digital sårbarhet – sikkert samfunn* og Meld. St. 38 (2016-2017) *IKT-sikkerhet. Et felles ansvar.* I internasjonal faglitteratur brukes i hovedsak begrepet forsyningskjede (Supply Chain), selv om Value Chain også unntaksvis forekommer. Begrepene synes i slike tilfeller å ha omtrent samme innhold.

KAPITTEL

# 02

# Risiko og sårbarhet i digitale verdikjeder

Sårbarheten i systemer har blant annet sammenheng med graden av avhengighet mellom de ulike leddene i verdikjedene systemene bygger på. Et system eller en verdikjede kan være kjennetegnet av tette eller løse koblinger. I et system som er preget av svært tette koblinger, vil en hendelse utløse andre følgehendelser umiddelbart, noe som gjør det vanskelig eller umulig å stoppe hendelsesforløpet.[3]

Systemenes kompleksitet har også betydning for sårbarheten. Komplekse systemer er uoversiktlige med mange aktører og et fragmentert systemansvar. Såkalt interaktiv kompleksitet referer til ukjente, ikke-planlagte, ikke-forventede sekvenser av hendelser i et system.[4] I systemer som er interaktivt komplekse, vil feil kunne påvirke på måter som operatører eller eksperter ikke kan forutse eller forhindre. Dersom systemet er tett koblet, kan disse feilene komme ut av kontroll før man er i stand til å oppfatte omfanget av problemet og korrigere. Dette innebærer at i slike systemer kan tilsynelatende små feil gi store konsekvenser.[5]

## 2.1 EGENSKAPER VED DIGITALE VERDIKJEDER

Tett koplede og komplekse digitale verdikjeder har egenskaper som analoge verdikjeder ikke i samme grad har. Det er spesielt tre egenskaper ved digitale verdikjeder som medfører utfordringer i risikostyringssammenheng:

Feil propagerer momentant og noen ganger på uforutsigbare måter.

For de som leverer en tjeneste på toppen av slike verdikjeder, er det svært utfordrende å skaffe seg oversikt over hvilke sårbarheter tjenesten er eksponert for lenger ned i kjeden. Dette forsterkes av verdikjedenes flyktighet. Underleverandører kan raskt og enkelt erstattes av andre.

Enkelte tjenester, som internett-tilgang og transmisjonsfunksjonaliteten i ekom-nettet, inngår i svært mange slike verdikjeder, uten at de ansvarlige for disse tjenestene selv nødvendigvis har oversikt over hvilke samfunnsfunksjoner de er bærere av.

Slike egenskaper kan også gjenfinnes i andre verdikjeder enn de rent digitale. Spesielt vil strømleveranser inn i digitale verdikjeder ha den egenskapen at et bortfall i verste fall kan gi en momentan konsekvens for en kritisk samfunnsfunksjon. På den annen side er bortfall av strømforsyningen en hendelse man kan sikre seg mot gjennom reservestrømforsyning fra batteribank eller aggregat.

Digitale verdikjeder er transnasjonale. Dette innebærer at ulike deler av verdikjeden er underlagt ulike staters jurisdiksjon, og at norske myndigheter derfor i begrenset grad kan ha kontroll over sikkerheten i leveranser av kritisk viktige varer og tjenester. De digitale verdikjedenes kompleksitet og den momentane propageringen av feil i slike kjeder, gjør at utfordringene knyttet til kjedenes grenseoverskridende karakter er spesielt store.

## 2.2 BEHOV FOR OVERSIKT

Behovet for oversikt over en digital verdikjede vil avhenge av kritikaliteten til den funksjonen den understøtter. For et kommunikasjonsnett mellom nødetatene er slik oversikt langt viktigere enn for eksempel for en digital parkeringstjeneste.

Ulike aspekter ved den enkelte verdikjede påvirker sårbarhetsbildet, og disse må virksomhetene ta hensyn til i risikostyringsarbeidet. De aspektene som er viktigst i et sårbarhetsperspektiv er diskutert i separate avsnitt av dette kapittelet. Ingen av disse aspektene vil kunne analyseres uten at man først har skaffet seg en oversikt over de aktuelle digitale verdikjedene.

Eksempelet i boks 2.1 tydeliggjør en rekke av disse aspektene. Det benyttes derfor som en gjennomgående illustrasjon.

[3] Charles Perrow (1984, 2008).
[4] Alexander Bøe et. al. (2012).
[5] Ibid.

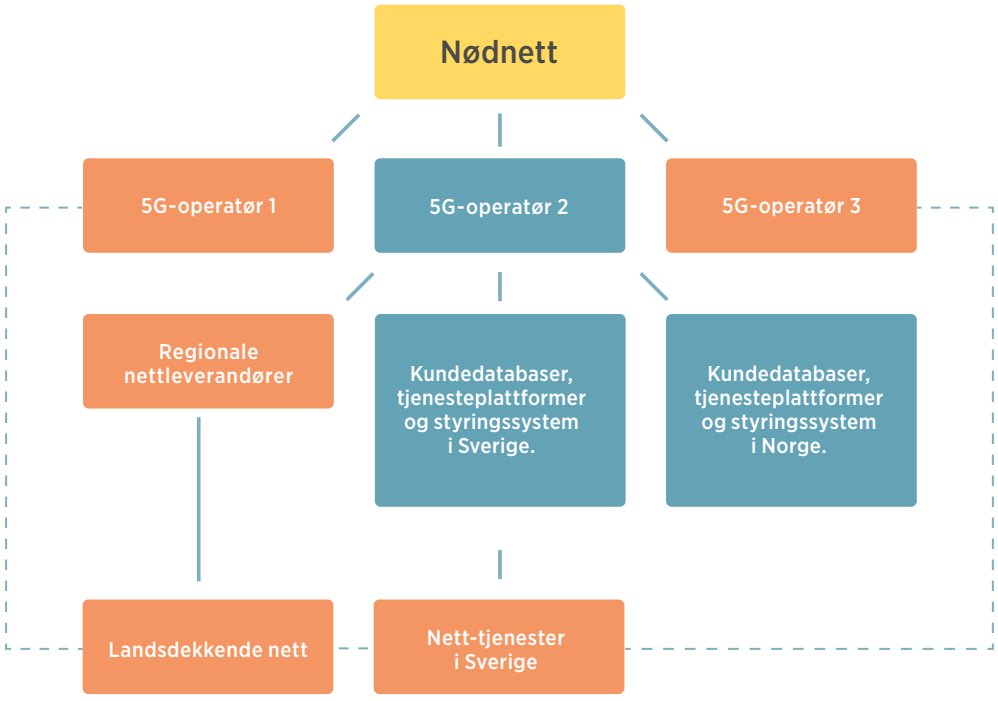
**Boks 2.1: Eksempel på digital verdikjede**

Det er besluttet at når første generasjons digitale Tetra-baserte nødnett skal fases ut, så skal det erstattes av et nett som kjøper nettilgang fra de kommersielle mobiltilbyderne. Det er en rekke forskjellige modeller for hvordan dette kan realiseres, og vi tar ikke stilling til hvilken som bør velges.
Vi benytter imidlertid en tenkt realisering av dette nødnettet ved hjelp av kommersielle tilbydere som et illustrativt eksempel på forskjellige sider av digitale verdikjeder.

Dersom nødnettet skal realiseres ved å kjøpe tjenester fra de fremtidige 5G-nettene til tre forskjellige mobil-operatører, vil alle disse operatørene inngå i den digitale verdikjedestrukturen til nødnettet.
Dette er illustrert i figuren under.

Hver av disse operatørene kan imidlertid kun levere tjenestene dersom de verdikjedene de selv er avhengige av leverer de tjenestene de skal. For en mobiloperatør vil det bety at alle de regionale nettleverandørene som 5G-basestasjonene er koblet til, leverer det de skal. Disse regionale nettene er i sin tur avhengige av at det landsdekkende nettet som de er tilkoblet, fungerer. Uten at denne forutsetningen er tilstede, vil de regionale nettene svikte.

Videre er 5G-operatøren avhengig av at flere systemer samvirker for at basestasjonene skal kunne virke som de gjør. Kundedatabaser, tjenesteplattformer og styringssystemer er helt nødvendige for at 5G-nettet skal virke, og derfor for at operatøren skal kunne levere tjenesten sin til nødnettet. For enkelhets skyld er dette kun illustrert for operatør 2 i figuren. I figuren har vi også gjort en antagelse om at 5G-operatør 2 har sitt hovedkontor i Sverige. Kundedatabaser, tjenesteplattformer og styringssystemer er derfor lokalisert der, og disse er derfor også avhengige av nett-tjenester i Sverige. Norske krav gjør imidlertid at 5G-nettet i en nødsituasjon også skal kunne driftes fra Norge. Det finnes derfor et duplisert sett av slike systemer som ligger her i landet.



## 2.3 HVORDAN SER EN FULLSTENDIG OG DETALJERT DIGITAL VERDIKJEDE UT?

Verdikjeden i boks 3.1 er tegnet på et aggregert nivå. Dette gjør oppgaven med å fremstille kjeden overkommelig, men på den annen side er det mye som er utelatt. Spesielt er det to dimensjoner vi ikke har tatt med:

*Tjenester kontra hardware og software*. I figuren har vi konsentrert oss om en kjede der de digitale leveransene mellom virksomhetene er tjenester. Det betyr at for en 5G-operatør har vi tegnet inn avhengigheten til tjenester fra regionale nettleverandører samt tjenesteleveranse fra kundedatabaser, tjenesteplattformer og lignende.

Leveranser av komponenter i hardware og software er utelatt i figuren, men det vil være omfattende leveransekjeder knyttet til slike digitale produkter også. En 5G-leverandør vil for eksempel være avhengig av hardware- og softwareleveranser fra Ericsson, Nokia eller Huawei både til basestasjonene sine og til noe av softwaren som kjører i bakgrunnen. De vil også være avhengige av tjenester fra en av disse, for at lisensene for basestasjonene til enhver tid skal være oppdaterte.

Disse tre selskapene vil i sin tur være avhengige av underleverandører for komponenter til sine hardware- og softwareprodukter. Disse underleverandørene vil være selskaper som leverer mindre softwarekomponenter, kretskort og integrerte kretser, selskaper som leverer utviklingsverktøy slik som kompilatorer og synteseverktøy, og av virksomheter som fabrikkerer hardware basert på spesifikasjoner gitt av disse selskapene.

*Virksomhetsnivå kontra utstyrsnivå*. Figuren forholder seg i hovedsak til virksomheter. Internt i hver virksomhet vil det imidlertid være en rekke systemer som leverer tjenester til hverandre. Dette er i noen grad illustrert gjennom de tre blå rektanglene i figuren, hvor det vil være naturlig å tenke seg at kundedatabaser, tjenesteplattformer og styringssystem er operert av samme virksomhet som er omtalt som «5G-operatør 2» i figuren. Det fulle bildet vil imidlertid være langt mer komplekst enn dette. Internt i virksomheten vil det være nettverk, det vil være kjølesystemer, og det vil være redundans i sentrale komponenter. Både de regionale nettleverandørene og den landsdekkende nettleverandøren vil ha installasjoner på et antall steder, og de vil ha fiberforbindelser imellom disse stedene. Disse fiberforbindelsene vil i mange tilfeller være leid av andre virksomheter.

Diskusjonen over gjør det klart at den verdikjeden som i eksempelet skal understøtte det tenkte nødnettet, er svært omfattende, og et konservativt estimat kan være at en full analyse av kjeden vil kunne lede frem til et firesifret antall elementer. Til tross for at det for enkelte svært kritiske anvendelser vil være ønskelig med komplett oversikt over hvordan sårbarheter propagerer i en verdikjede, er det i dagens situasjon urealistisk å fremskaffe dette. Til det er den totale digitale verdikjeden som inkluderer leveranser av tjenester, hardware og software, og som dekker den fulle kompleksiteten av dette internt i hver virksomhet, for omfattende. Et sentralt element i arbeidet med digitale verdikjeder må derfor være å balansere ressursbruk mot behovet for detaljert oversikt.

## 2.4 FALSK ELLER SVEKKET REDUNDANS

En betydelig motivasjon for å fremskaffe oversikt over digitale verdikjeder er knyttet til falsk eller svekket redundans. Begrepet beskriver tilsynelatende redundante løsninger som deler sårbarheter lenger ned i verdikjeden. Et eksempel på dette kan gjenfinnes i figuren i boks 3.1.

Det er lagt opp til redundans i nødnettet ved at det er tre operatører som alle skal levere den nettjenesten nødnettet er avhengig av. Den redundansen som dette gir, blir imidlertid svekket av at de alle tre har en absolutt avhengighet av det samme landsdekkende

nettet. Redundansen gir fremdeles verdi i den forstand at utfall av en eller to operatører ikke hindrer nødnettet i å fungere. Den er imidlertid ikke absolutt, siden et utfall i det landsdekkende nettet vil kunne ta ned alle de tre operatørene. Den avtalestrukturen som nødnettet har med de tre operatørene, gir derfor en redundans som kun kan analyseres dersom man har oversikt over flere ledd i verdikjeden.

## 2.5 FORSKJELLIGE FORMER FOR AVHENGIGHET

Den visuelle fremstillingen av den digitale verdikjeden til det tenkte nødnettet i boks 3.1 inneholder ikke all informasjon som er nødvendig for å kunne gjøre en sårbarhetsanalyse. Dette er tydeligst der hvor operatør 2 har tre elementer under seg, og som vi derfor skulle anta at den er avhengig av for å kunne levere tjenestene sine. Disse tre elementene spiller imidlertid forskjellige roller i et avhengighetsperspektiv.

Kundedatabaser, tjenesteplattformer og styringssystem i Sverige og Norge dupliserer hverandre og gir redundans. Operatøren er i stand til å operere dersom kun én av dem er operativ. Avhengigheten av regionale nettverk, og den avhengigheten av et landsdekkende nett som følger av dette, er imidlertid av en annen karakter, selv om dette ikke fremgår av figuren. Operatør 2s 5G-nett vil kunne operere på full kapasitet dersom *alle* de regionale nettene opererer på full kapasitet, og i tillegg at *enten* systemene i Sverige *eller* systemene i Norge opererer på full kapasitet. En oversikt over digitale verdikjeder må derfor kunne fange inn forskjellen mellom redundans og absolutt avhengighet.

## 2.6 KONFIDENSIALITET, INTEGRITET OG TILGJENGELIGHET

I arbeidet med å utvikle en modell for risikostyring i digitale verdikjeder legger arbeidsgruppen til grunn samme forståelse av sikkerhetsmålene for digital sikkerhet som det IKT-sikkerhetsutvalget gjorde:

Tilgjengelighet, dvs. at IKT-systemene, informasjonen som behandles i systemene og tjenestene tilknyttet systemene, er tilgjengelig der - og når – brukerne trenger dem

Integritet, dvs. at IKT-systemene, informasjonen som behandles i systemene og tjenestene tilknyttet systemene, ikke endres utilsiktet eller uautorisert

Konfidensialitet, dvs. at IKT-systemene, informasjonen som behandles i systemene og tjenestene tilknyttet systemene, kun er tilgjengelige for dem som rettmessig skal ha tilgang til dem[6]

Risikovurderinger basert på verdikjeder vil se forskjellig ut avhengig av hvilket sikkerhetsmål man tar utgangspunkt i. Redundans vil for eksempel være et ubetinget gode dersom tilgjengelighet er det eneste sikkerhetsmålet man er opptatt av. Redundans representerer imidlertid en økning i angrepsflate, og derfor en øket sårbarhet dersom det er konfidensialitet som har hovedprioritet. Dersom det er integritet som er den største bekymringen, kan redundans i noen tilfeller være en styrke dersom den er innrettet slik at integritetsbrudd kan oppdages, for eksempel ved at det registreres avvik mellom innholdet i de redundante systemene. Hvis redundansen er innrettet slik at den ikke vil oppdage integritetsbrudd, vil redundans kunne representere en øket sårbarhet også for integritetsbrudd.

Brudd på integritet og konfidensialitet er absolutte størrelser i den forstand at et brudd enten foreligger eller ikke foreligger; det finnes ingen mellomting. Brudd på tilgjengelighet kommer imidlertid i mange forskjellige former, og hvorvidt det faktisk foreligger et brudd, vil ofte være et spørsmål om skjønn.

[6] NOU 2018: 14 *IKT-sikkerhet i alle ledd.*

Eksempelvis kan en tjeneste få redusert ytelse på flere måter:

Den kan få redusert kapasitet. For eksempel vil redusert kapasitet fra en kundedatabase kunne føre til at det er færre mobiloppkoblinger som aksepteres. Mobilnettet vil fremdeles virke, men det vil gi inntrykk av å være overbelastet selv om det er mye ledig kapasitet. Hvorvidt det foreligger et brudd på tilgjengelighet, må vurderes med utgangspunkt i graden av overbelastning.

Tjenesten kan få økt responstid. For eksempel kan økt responstid og forsinkelse være helt ødeleggende for en telefonsamtale, og den vil likeledes kunne føre til at banktjenestene er utilgjengelige dersom bankens maskiner gir opp ventingen før Bank-ID responderer. For andre anvendelser – slik som overføring av trafikkovervåkningsdata – kan det tenkes at økt responstid ikke har noen merkbar negativ effekt.  Hvorvidt det foreligger et brudd på tilgjengelighet, vil i denne sammenhengen avhenge av hvilke anvendelser man vektlegger, og hvordan de er rammet.

Tjenesten kan være ustabil. En ustabil nettverksforbindelse som er nede i et halvt sekund per minutt, vil for noen anvendelser være helt ødeleggende, mens de for andre anvendelser ikke vil være merkbare. Eksempelvis kan en tjeneste som GPS komme og gå dersom den blir utsatt for jamming. Også her vil det være et spørsmål om skjønn om det foreligger brudd på tilgjengelighet.

Tjenesten kan ha geografisk begrensede bortfall. Dette vil for eksempel kunne skje dersom et uhell gjør at mobile basestasjoner faller bort i et område. Et geografisk utfall av nettverkstjenester som er lokalisert til et hyttefelt, vil være av begrenset betydning, mens et utfall i en større by vil kunne være alvorlig.

Alle disse formene for brudd vil kunne ha forskjellig betydning for de tjenestene de bygger opp under. Problemer som oppstår ett sted i kjeden, kan nemlig endre karakter mens de propagerer oppover i kjeden. Denne endringen i karakter kan i noen tilfeller gjøre at reelle problemer ett sted ikke er merkbare lenger oppe i kjeden. Andre ganger kan et tilsynelatende ubetydelig problem ett sted føre til et komplett bortfall av en viktig digital funksjon.

Spesielt viktig er det å merke seg at verken konfidensialitets- eller integritetsbrudd nødvendigvis må fremstå som brudd av samme karakter lengre opp i verdikjeden. Et passord på avveie hos en leverandør med driftsansvar for et annet selskaps systemer er et konfidensialitetsbrudd hos leverandøren. Det kan imidlertid føre til uautoriserte endringer i data hos mottakeren av tjenesten, noe som medfører et integritetsbrudd. Dersom dette integritetsbruddet gjør at selskapets systemer slutter å virke, vil det kunne føre til et tilgjengelighetsbrudd for selskapets kunder. Dette eksempelet viser at selv om den digitale verdikjeden angir at problemer vil propagere fra en virksomhet til en annen, er måten problemet vil propagere på, avhengig av en rekke faktorer. Disse faktorene må tas hensyn til i arbeidet med digitale verdikjeder.

## 2.7 VERDIKJEDER SOM GÅR UT AV LANDET

Tre faktorer kan bidra til at verdikjeder som understøtter kritiske funksjoner, får forgreninger som går ut av landet. Den mest åpenbare er knyttet til beslutninger om kjøp av digitale tjenester fra aktører som ligger i andre land. Disse tjenestene kan eksempelvis være driftstjenester eller skytjenester. I svært mange tilfeller er slike tjenester gjenstand for et eksplisitt kjøp og en eksplisitt beslutning om å legge en forgrening av verdikjeden utenlands. Det finnes imidlertid tilfeller hvor den utenlandske forgreningen er en mer implisitt del av kontrakten. Eksempelvis er det vanlig at software forhandles som lisenser som gir rett til bruk av produktet. I mange tilfeller vil selve lisenstjeneren – den maskinen som sjekker om du har en gyldig lisens – ligge utenfor landets grenser. En slik situasjon vil føre til en kritisk avhengighet som går ut av landet.

Den andre faktoren er knyttet til at internettets arkitektur vanskeliggjør nasjonal kontroll. Et godt eksempel er Border Gateway Protocol (BGP) som er den strukturen som kobler alle deler av internett sammen til en felles stor infrastruktur. BGP er en

helt nødvendig komponent for å få nettbaserte anvendelser til å virke og er bygget opp ved hjelp av en global struktur av maskiner som gjensidig påvirker hverandre. Dette gjør det mulig for en maskin i utlandet å påvirke i hvilken grad en datatjeneste Norge er tilgjengelig.

Den tredje faktoren er direkte knyttet til hardware og software. Det finnes få, om noen, elektroniske produkter hvor både hardware og software er fullt ut produsert i Norge ved hjelp av verktøy som også fullt ut er utviklet i Norge.

Summen av disse tre faktorene gjør at det knapt finnes en digital verdikjede som ikke har kritiske forgreninger som går ut av landet. Disse forgreningene representerer spesielle utfordringer. Den mest åpenbare av disse er at de virksomhetene som inngår i utenlandske forgreninger i begrenset grad vil være underlagt norsk jurisdiksjon. Norsk lovverk og norske reguleringsregimer alene vil derfor i begrenset grad kunne benyttes til å fremskaffe full oversikt over verdikjedene.

KAPITTEL

# 03

# Modell for risikostyring på virksomhetsnivå

Arbeidet med å redusere risiko og sårbarhet knyttet til virksomhetens digitale verdikjeder, må inngå i virksomhetens ordinære risikostyringsprosess, som igjen bør være en integrert del av ledelse og beslutningstaking i virksomheten som helhet.

Modellen vi beskriver i dette kapitlet er innrettet mot virksomheter, men skal også kunne tjene behovene til forskjellige myndighetsaktører. For myndighetene kan modellen danne utgangspunkt for så vel regulering som for mykere governance-tiltak, jf. kapittel 5.

Modellen er rettet inn mot kartlegging av avhengigheter mellom virksomheter. Bare i den grad det er nødvendig for å tydeliggjøre ansvarsforholdet virksomhetene imellom, tar modellen for seg enkeltstrukturer i hver enkelt virksomhet.

Begrepene kunde, leverandør og underleverandør benyttes slik de er beskrevet i punkt 2.2.4.

For enkelte deler av ekomsektoren vil det forekomme såkalte *peering-avtaler*, hvor begge parter spiller rollen som kunde og leverandør. I modellen skal en peering-partner behandles både som en kunde og som en leverandør.

## 3.1 EGENSKAPER VED MODELLEN

Modellen skal for det første *gi veiledning* i hvordan en virksomhets interne risiko- og sårbarhetsvurdering *kan fange opp sårbarheter* som propagerer gjennom komplekse digitale verdikjeder. Dette betyr at den må gi rammer for å vurdere behovet for oversikt over de underliggende verdikjedene basert på kritikaliteten til de tjenestene som virksomheten tilbyr.

For de fleste virksomheter vil behovet begrense seg til oversikt over leverandørene i første ledd og den Service Level Agreement (SLA) disse har med hver underleverandør. Kun for viktige tjenester vil det kreves en oversikt lengre ned i kjeden.

For det andre skal modellen hjelpe virksomheter i å skaffe seg *oversikt over egne leverandører og deres underleverandører som utgangspunkt for vurdering av risikoreduserende tiltak*. Modellen må skissere en prosess for fremskaffelse av informasjon om leverandørers verdikjeder. Dersom resultatet av prosessen ikke står i forhold til den eksplisitt formulerte risikoaksepten, må enten risikoaksepten reformuleres, eller det må iverksettes tiltak.

For det tredje skal modellen gi *oversikt over hvilke digitale verdier i form av sluttleveranser virksomheten er ansvarlig for*. Summen av de verdiene kundene samlet stiller en virksomhet ansvarlig for, kan tilsi større oppmerksomhet om sikkerhet enn det som rettferdiggjøres av krav stilt fra en enkeltkunde.

Ideelt sett har en virksomhet egeninteresse av å håndtere sårbarhet gjennom økt ressursbruk på sikkerhet. Der hvor det ikke er tilfellet, bør regulatoriske virkemidler vurderes.

## 3.2 RISIKOSTYRINGS-PROSESSEN

Arbeidet med å skaffe oversikt over og styre risikoen i digitale verdikjeder er en kontinuerlig prosess som må gjentas regelmessig og spesielt ved endringer i forhold som kan påvirke risikoen og sårbarheten.

Risikostyringsprosessen kan deles inn i fem trinn med tilhørende spørsmål som må besvares. Det er en logisk rekkefølge mellom trinnene, og vurderingene og svaret på det første spørsmålet avgjør om det er behov for å arbeide med de fire neste.

En kort sammenfatning av de fem trinnene er som følger:

*1. Omfang og kontekst – behov for oversikt over digitale verdikjeder*

- Er det nødvendig å få oversikt over den digitale verdikjeden som virksomhetens leverandører er avhengig av?

- Hvilke interne og eksterne kontekstuelle forhold bør tas med i betraktning når videre vurderinger skal gjøres?

*2. Risikoidentifisering – informasjonsinnhenting*

- Dersom svaret på det første spørsmålet over er «ja», fra hvilke leverandører bør virksomheten innhente denne oversikten?
- Hvor langt ned i kjeden er det ønskelig og mulig å skaffe oversikt, og hvilke opplysninger bør leverandørene bes om å fremskaffe?

*3. Risikoanalyse*

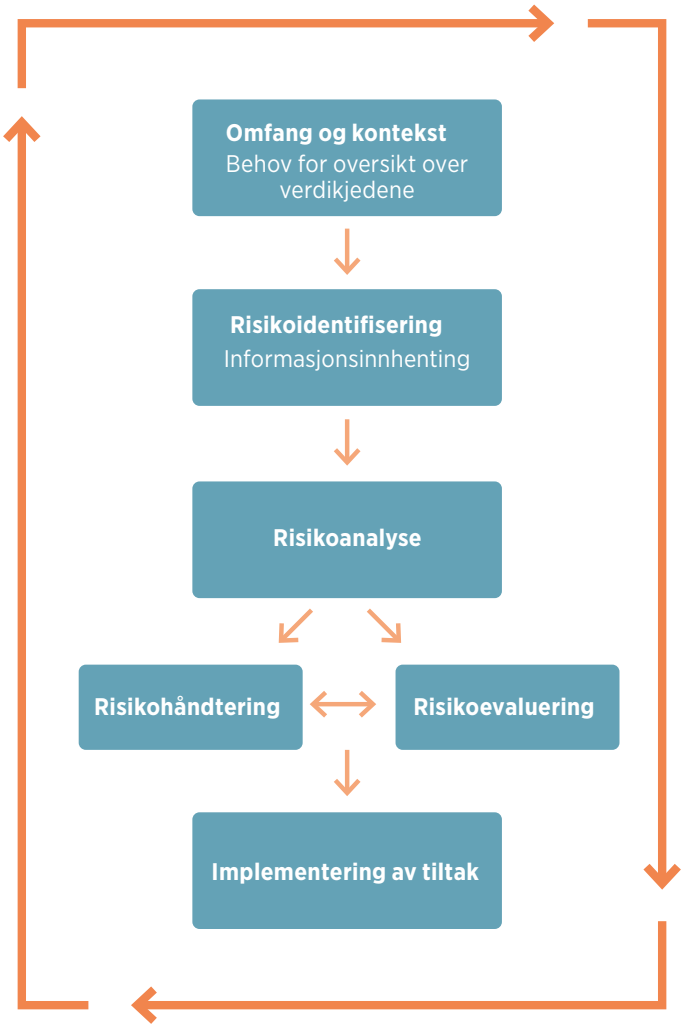
- På bakgrunn av de innhentede opplysningene, hvordan vurderer virksomheten risiko knyttet til hendelser i verdikjeden?
  - Hvor sannsynlig er slike hendelser?
  - Hvilke konsekvenser kan de få?
  - Hvor sikre er man på disse vurderingene?

*4. Risikoevaluering og risikohåndtering*

- I hvor stor grad er virksomheten villig til å akseptere den risikoen som er avdekket?
- Hvor stort er potensialet for risikoreduksjon?
- Hvilke tiltak kan redusere risikoen til et (mer) akseptabelt nivå?
- Er disse tiltakene forsvarlige ut fra en nytte/kostnadsvurdering og positive og negative bieffekter av tiltaket?

*5. Implementering av tiltak*

- Hvordan skal tiltak implementeres og følges opp?




**FIGUR 3.1:** Risikostyring i digitale verdikjeder

En mer detaljert beskrivelse av hvert enkelt trinn følger i punktene 3.2.1. – 3.2.4. under. Trinnene vil samlet sett gi en prosess som illustrert i figur 4.1. Figuren er basert på en generell modell for risikostyring (jf. NS-ISO 31000:2018), men er forenklet og tilpasset arbeidet med digitale verdikjeder.

Digitale verdikjeder er dynamiske av natur og vil kunne endres som følge av kommersielle eller kontraktsmessige forhold. Implementering av risikoreduserende tiltak kan også ha som et direkte eller indirekte resultat at den digitale verdikjeden forandres. Oversikten over verdikjedene må derfor løpende holdes ved like.

### 3.2.1 OMFANG OG KONTEKST – IDENTIFISERE BEHOV FOR KARTLEGGING AV DIGITALE VERDIKJEDER

Når er det nødvendig å kartlegge digitale verdikjeder?
Dersom myndigheter eller kunder krever at virksomheten skal ha oversikt over digitale verdikjeder, må virksomheten fremskaffe slik oversikt. Virksomheten kan imidlertid også ha behov for dette selv om slike krav ikke foreligger. Dette kan være fordi forretningsmessige hensyn og/eller virksomhetens samfunnsmessige betydning tilsier det. Se tabell 3.1 under.

Når bør virksomheten kartlegge verdikjeder selv om den ikke er forpliktet til det?
Behov for kartlegging av digitale verdikjeder vil, dersom det ikke foreligger et eksternt krav om dette, avhenge av verdikjedenes betydning for egen forretningsdrift eller for ivaretakelse av virksomhetens samfunnsansvar.

I en slik vurdering er det ikke bare verdikjedenes betydning som må tillegges vekt, men også virksomhetens inntrykk av om det kan foreligge en uakseptabel sårbarhet knyttet til verdikjedene, og dessuten andre ytre forhold som kan tilsi at det foreligger en uønsket risiko. Informasjon om trussel- og sårbarhetsbildet fra relevante myndigheter kan her være viktig.

Vurderingen forutsetter at det gjennomføres en innledende enkel prosess for å avklare om det er behov for å gå videre og sette i gang en kartlegging av digitale verdikjeder. Virksomheten må ta stilling til i hvilken grad det sårbarhetsbildet man oppfatter, er akseptabelt, og om den kunnskapen man baserer dette på er tilstrekkelig.

| Vurderingselementer | Hovedspørsmål | Kommentar |
|---|---|---|
| **Krav fra myndigheter** | Foreligger det krav om oversikt over digitale verdikjeder fra myndigheter? | Myndighetene stiller per i dag ikke eksplisitte krav om oversikt over digitale verdikjeder ut over sikkerhetslovens krav om kartlegging av direkte avhengigheter. Ytterligere krav kan imidlertid komme gjennom endringer i lovverket, eller ved innføring av nye reguleringer. |
| **Krav fra kunder** | Foreligger det krav om oversikt over digitale verdikjeder fra kunder? | Et slikt krav bør være kontraktsfestet. Hos kunden vil et slikt krav være et resultat av kundens eget arbeid med digitale verdikjeder, og kravet følges typisk av et krav om at oversikt over verdikjeden skal rapporteres til kunden. |
| **Kritikalitet for egen forretningsdrift** | I hvilken grad er det behov for oversikt over digitale verdikjeder av hensyn til egen forretningsdrift? | Se neste tabell |
| **Kritikalitet for samfunnet** | I hvilken grad gir virksomhetens samfunnsansvar grunn til å skaffe seg oversikt over digitale verdikjeder? | Se neste tabell |

**TABELL 3.1:** Når er det nødvendig å kartlegge digitale verdikjeder?

I tabell 3.2 under gjengis hjelpespørsmål som kan brukes i vurderingen av om virksomheten bør kartlegge verdikjeder selv om den ikke er forpliktet til det.:

| Vurderingselementer | Hovedspørsmål | Kommentar |
|---|---|---|
| **Verdikjedens kritikalitet for egen virksomhet** | Hvor vesentlig er den digitale verdikjeden for virksomhetens totale leveringsdyktighet? | Dersom virksomheten vurderer at avhengigheten av en underleverandør er så stor at egen leveringsevne i alvorlig grad kan rammes ved en hendelse i verdikjeden, tilsier dette at det er behov for oversikt. Det samme er tilfellet dersom en slik hendelse kan ramme virksomhetens tillit i markedet. Dette kan omfatte så vel tilgjengelighet som konfidensialitet og integritet. |
| **Verdikjedens kritikalitet for samfunnet** | Hvor vesentlig er den digitale verdikjeden for virksomhetens ivaretakelse av eget samfunnsansvar? Hvor viktig er den digitale verdikjeden for andre aktørers ivaretakelse av sitt samfunnsansvar? | Samfunnsansvaret kan innbefatte både direkte leveranser til samfunnet og de samfunnsmessige verdier virksomhetens leveranser samlet bærer. Ivaretakelse av samfunnsansvar har selvsagt også betydning for virksomhetens tillit hos myndigheter og kunder og kan derfor ikke betraktes helt adskilt fra vurderingen av hva som er forretningsmessig forsvarlig. |
| **Trusselbildet** | Er det forhold som tilsier at verdikjeden kan være særlig utsatt for subversjon, sabotasje eller spionasje? | Dersom trusselbildet generelt tilsier det, eller den sektoren virksomheten og/eller dens leverandører tilhører er spesielt utsatt for sikkerhetstruende virksomhet, gir dette grunn til å kartlegge verdikjeden. |
| **Behov for oversikt over falsk eller svekket redundans** | Hvor reell er den etablerte redundansen? | Dersom alternative løsninger er etablert for å sikre tilgjengelighet eller håndtere integritetsbrister, taler dette for at virksomheten bør skaffe seg oversikt over de digitale verdikjedene for å undersøke hvor reell redundansen er. |
| **Hvem har tilgang til kritiske informasjon?** | I hvilken grad har virksomheten behov for å skaffe seg oversikt over hvem som får virksomhetens kritiske informasjon i hende? | Dersom virksomheten overlater egen kritisk informasjon til en leverandør, taler dette for at virksomheten bør skaffe seg oversikt over de digitale verdikjedene. Dette for å fremskaffe en oversikt over hvilke andre virksomheter som får tilgang til informasjonen. |
| **Hvem er i posisjon til å endre data som virksomheten er ansvarlig for?** | I hvilken grad har virksomheten behov for å skaffe seg oversikt over hvem som er i posisjon til å endre data som den er ansvarlig for? | Dersom virksomheten benytter en leverandør på en slik måte at kritiske data kan endres, taler dette for at virksomheten bør skaffe seg oversikt over de digitale verdikjedene. |
| **Graden av tillit til leverandører eller underleverandør** | I hvilken grad har virksomheten tillit til leverandør og/eller underleverandøren? | Dersom virksomheten opplever at det er et misforhold mellom de verdiene som må tiltros (under)leverandøren og den tillit (under) leverandøren har, taler dette for at virksomheten bør skaffe seg oversikt over leverandørens digitale verdikjeder. |
| **Insitament** | I hvilken grad har virksomheten tillit til at kontrakten samlet sett gir tilstrekkelig insitament for leverandøren til å levere sikre og robuste løsninger? | Dersom virksomheten vurderer at den kontrakten man har med en leverandør ikke gir leverandøren tilstrekkelig insitament til å investere i trygg leveranse av digitale tjenester, taler dette for at virksomheten bør skaffe seg oversikt over leverandørens digitale verdikjeder. |

**TABELL 3.2:** Når bør virksomheten kartlegge verdikjeder selv om den ikke er forpliktet til det?

Hvis ingen krever oversikt over virksomhetens digitale verdikjeder, og virksomheten selv aksepterer risikoen knyttet til disse verdikjedene, foreligger det ikke et behov for å skaffe oversikt over de digitale verdikjedene.

I motsatt fall må virksomheten starte kartleggingsprosessen.

### 3.2.2 RISIKOIDENTIFISERING – INFORMASJONSINNHENTING

Under dette punktet er det to forhold som skal kartlegges:

- *Hvilke* leverandører skal virksomheten be om informasjon fra?
- *Hva* skal leverandører gi informasjon om?

| Vurderingselementer | Hovedspørsmål | Kommentar |
|---|---|---|
| **Tilgjengelighet** | I hvilken grad kan leverandøren sette virksomheten i en situasjon hvor den digitale tjenesten/produktet den leverer får merkbart redusert ytelse? | Med «ytelse» menes her det antallet operasjoner tjenesten eller produktet kan håndtere per tidsenhet. Dette kan eksempelvis være antallet oppslag per sekund i en database. |
| | I hvilken grad kan leverandøren sette virksomheten i en situasjon hvor den digitale tjenesten/produktet den leverer får merkbart økt forsinkelse? | Med forsinkelse menes her den tiden det går fra en digital operasjon blir bestilt til den er gjennomført. For en kundedatabase kan dette være tiden det tar fra forespørsel om oppslag er mottatt, til resultatet av oppslaget er levert. |
| | I hvilken grad kan leverandøren sette virksomheten i en situasjon hvor den digitale tjenesten den leverer faller bort, eller det produktet den selger ikke kan leveres? | Merk at både økt forsinkelse og redusert ytelse hos en leverandør eller underleverandør kan ha den konsekvensen at egen tjeneste faller bort. I noen sammenhenger har omfang og lokalisering av utfall betydning for i hvilken grad det er akseptabelt eller ikke. Se omtale under tabellen. |
| **Konfidensialitet** | Får leverandøren tilgang til data som har konfidensialitetskrav til seg? | Data som har konfidensialitetskrav til seg, kan stamme fra virksomhetens kunder, fra myndigheter eller fra virksomhetens egen forretningsdrift. |
| | I hvilken grad vil de krypteringsløsningene virksomheten benytter kunne beskytte de av virksomhetens data som leverandøren og eventuelt underleverandører får tilgang til? | Her må det gjøres en vurdering av styrken til de krypteringsløsningene som er implementert for å sikre den informasjonen som leverandører og underleverandører får i hende. Videre må det gjøres en vurdering av trusselbildet, dvs. hvem som har illegitim interesse av å få tak i dataene, og hvilke kapabiliteter de har til å komme rundt krypteringen. |
| **Integritet** | Gjøres leverandøren ansvarlig for integriteten til virksomhetens data? | Data som har integritetskrav til seg, kan stamme fra virksomhetens kunder, fra myndigheter eller fra virksomhetens egen forretningsdrift. |
| | I hvilken grad vil de krypteringsløsningene og den redundansen virksomheten har på plass, gjøre at virksomheten oppdager, og eventuelt kan rette opp i integritetsbrudd som skjer via en leverandør eller underleverandør? | Dette spørsmålet skal avdekke om integriteten til de data som underleverandøren gjøres ansvarlig for, er rent tillitsbasert, eller om det finnes mekanismer som kan oppdage og rette opp i integritetsbrudd. |

**TABELL 3.3:** Hvilke underleverandører skal kartlegges?

Prinsippet er at den kartleggende virksomheten forholder seg til sine leverandører, som så igjen innhenter informasjon fra sine leverandører og så videre. Slik kartlegges kjeden steg for steg. Kontakten mellom partene som står i et avtalemessig forhold til hverandre, må være dialogbasert. Slik kan også underleverandører få et bilde av hvilke verdier deres virksomhet er bærere av.

Hvilke underleverandører skal kartlegges?
For å besvare dette spørsmålet må virksomheten ta utgangspunkt i hvilke leverandører som kan påvirke den tjenesten virksomheten selv leverer.

I tabell 3.3 under listes de delspørsmål om leverandøren som samlet sett er avgjørende for om underleverandører skal kartlegges.

Det er sentralt at alle leverandører og underleverandører som kartlegges i en verdikjede, mottar informasjon om hvem som har kartlagt dem. På den måten vil en underleverandør selv kunne danne seg et bilde av hvilke samfunnsverdier den er ansvarlig for.

Noen tjenester skal dekke en befolkning eller en kundemasse, og for slike tjenester vil problemer hos enkelte leverandører eller underleverandører kun ha effekt for en del av befolkningen/kundemassen. Hvorvidt leverandøren eller underleverandøren skal inngå i en oversikt over digitale verdikjeder, vil avhenge av i hvilke, og i hvor store, geografiske områder den digitale tjenesten kan påvirkes.

I slike tilfeller bør virksomheten vurdere:

- I hvilke geografiske områder/på hvilke lokasjoner påvirker (under)leverandørens tjenester ytelsen, forsinkelsen eller tilgjengeligheten til virksomhetens egne tjenester?
- For hvor stor del av befolkningen/kundemassen påvirker (under)leverandøren ytelsen, forsinkelsen eller tilgjengeligheten til virksomhetens egne tjenester?

Hva skal leverandørene gi informasjon om?
De leverandørene som virksomheten beslutter skal inngå i kartleggingen, bør bes om å rapportere oversikt over egne digitale verdikjeder til virksomheten. Dette fører i sin tur til at leverandørene må innhente informasjon fra egne leverandører og be om at disse igjen gjør tilsvarende henvendelser til sine.

Informasjonen bør minimum bestå i en identifikasjon av underleverandører, hvilket land de er registrert i, og hvilken tjeneste de leverer inn i verdikjeden. Andre aspekter som kan være relevante i enkelte situasjoner, er geografisk lokasjon til det utstyret underleverandøren benytter til å levere tjenesten, hvilke eiere underleverandøren har, underleverandørens økonomiske situasjon og klareringskrav til personell som kommer i kontakt med utstyret.

Virksomheten må for egen del ha oversikt over hvilke avtaler som er inngått med leverandøren blant annet med hensyn til tjenestenivå (SLA), og hvilke erfaringer virksomheten har med leverandøren og dens underleverandører. Dessuten må virksomheten ha et bilde av hvem som er avhengig av virksomhetens egne leveranser, og hvordan svikt vil påvirke kundene og samfunnet.

### 3.2.3 RISIKOANALYSE

Virksomheten bør gjøre en vurdering av hvilke trusler og farer som kan ramme egen virksomhet eller leverandørers og underleverandørers virksomhet. Det vil si å kartlegge hvilke utilsiktede og tilsiktede hendelser som kan inntreffe. I hvilken grad er verdikjeden utsatt for oppmerksomhet fra kriminelle og/eller fremmed etterretning? Trusselvurderinger, graderte og ugraderte, vil være en viktig informasjonskilde her. Er verdikjeden utsatt for naturfarer, graveskader osv.?

Når denne analysen og informasjonen fra leverandørene foreligger, starter selve analysearbeidet. Analysen bør avklare hvor trolig det er at det skal inntreffe hendelser i de ulike leverandørenes verdikjeder som kan ramme egen virksomhets interesser, og hvor alvorlige konsekvensene av hendelsen kan bli.

Risikoanalysen kan gjennomføres på ulikt vis. For tilsiktede handlinger som kan ramme virksomheten eller verdikjeden, kan en metode som baserer seg på en vurdering av verdi, sårbarhet og trussel anvendes.[7]

[7] Jf. f.eks. NSM (2016) og NS 5832:2014.

Verdi i denne sammenheng kan både være verdi for virksomheten, verdi for samfunnet og verdi for trusselaktørene. Disse verdivurderingene er ikke nødvendigvis sammenfallende. En leveranse av liten kommersiell betydning for virksomheten kan være viktig for samfunnet. En trusselaktør kan ha interesse av verdier ut fra helt andre hensyn enn deres samfunnsmessige betydning, for eksempel for å få tilgang til bedriftsintern informasjon eller bruke systemene som utgangspunkt for subversjonsaktiviteter.

En annen metode baserer seg på vurdering av sannsynlighet, konsekvens og usikkerhet.[8] Sannsynlighetsvurderingene kan bygge på en gjennomgang av de sårbarhetene, truslene og farene som er avdekket gjennom informasjonsinnhentingen sett opp mot hva som kan skje dersom leveransen svekkes eller bortfaller. Dette kan for eksempel gå på manglende eller svekket redundans, fare for konfidensialitetsbrudd, utilstrekkelig insitament for å opprettholde stabilitet i leveransene, avhengighet av utenlandsk infrastruktur og utenlandske eiere osv.

Konsekvensbildet må basere seg på en kartlegging av hvilke konsekvenser svikt i de digitale verdikjedene kan få for egen virksomhet, basert på verdiene som er identifisert. Hvor store tap medfører det, hvordan påvirker det samfunnet, hvor stort blir omdømmetapet for virksomheten, hvordan påvirker det arbeidssituasjonen for egne ansatte?

Gjennom risikoanalysen etableres det et risikobilde. Kvaliteten på risikobildet avhenger av kvaliteten på den informasjonen som er innhentet, og de vurderingene som er gjort. Virksomheten bør gjøre vurderinger av hvor godt kunnskapsgrunnlaget for analysen er, og hvor sensitivt utfallet er for mindre endringer i forutsetningene (for eksempel at en trusselaktør kan benytte seg av *innsidere* i et angrep på kjeden). Den usikkerheten som svakheter i kunnskapsgrunnlaget og sensitivitet i vurderingene utgjør, må tas med i de videre vurderingene av om den avdekkede risikoen er akseptabel eller ikke.

### 3.2.4 RISIKOEVALUERING OG RISIKOHÅNDTERING

Etter at virksomheten gjennom risikoanalysen har etablert et bilde av hvilken risiko som er knyttet til de digitale verdikjedene virksomheten er avhengig av, må virksomheten ta stilling til i hvilken grad denne risikoen er akseptabel eller ikke.

I denne evalueringen er det også nødvendig å se hen til hvilket potensial for risikoreduksjon som foreligger. Hvilke tiltak er mulige, hvilken effekt vil de ha og hva vil de koste? Tiltak kan ha positive og negative bieffekter som også må tas hensyn til i vurderingene.

I hvilken grad er den avdekkede risikoen akseptabel?
Etter å ha vurdert disse spørsmålene bør virksomheten stille kontrollspørsmålet om hvorvidt alle myndighetskrav eller kontraktsfestede krav til oversikt over digitale verdikjeder fra kunder er tilfredsstilt. Her må det spesielt vurderes om oversikten man sitter med er tilstrekkelig for å svare tilfredsstillende på spørsmålene i tabell 3.4.

I hvilken grad foreligger det et realistisk potensial for risikoreduksjon?
I vurderingen av om risikoen er akseptabel eller ikke, er det vanligvis nødvendig å se hen til hvilke realistiske muligheter som finnes for å redusere den. I begrepet "realistisk" ligger det her både en vurdering av hva som faktisk er mulig å få til, og hva som er forsvarlig ut fra en kost/nytte-vurdering og en vurdering av bieffekter.

I mange tilfeller vil det ikke være praktisk mulig å fremskaffe fullstendig oversikt over en underleverandørs digitale verdikjeder. Dette vil ofte (men ikke alltid) være tilfelle for leveranser av software og hardware, hvor en fullstendig oversikt over historien og opphavet til alle deler av produktet, samt de verktøy som er brukt i designet av produktet, ikke er mulig å fremskaffe. Dette vil også være vanskelig dersom leverandøren eller en underleverandør ikke er villig til å fremskaffe eller dele den nødvendige informasjonen. Det finnes imidlertid grader av

[8] Jf. f.eks. NS 5814:2008.

| Vurderingselementer | Hovedspørsmål | Kommentar |
|---|---|---|
| **Tilstrekkelig oversikt** | I hvilken grad er den oversikten over digitale verdikjeder som virksomheten har etablert, tilstrekkelig til å ta stilling til om risikoen knyttet til kjedene er akseptabel? | En fullstendig oversikt over digitale verdikjeder som inkluderer alle aspekter av både tjenester, hardware og software vil sjelden være mulig å fremskaffe. Den oversikten som foreligger vil derfor ofte være ufullstendig. |
| **Redundans** | I hvilken grad er den reelle redundansen i den digitale verdikjeden akseptabel for virksomheten? | Når virksomheten har benyttet seg av redundans som sikkerhetsmekanisme vil det være nødvendig å undersøke i hvilken grad redundansen er svekket nedover i verdikjeden. |
| **Tilgjengelighet** | I hvilken grad kan virksomheten akseptere den risikoen som er knyttet til hvem som er i posisjon til å påvirke ytelsen eller forsinkelsen til den tjenesten eller de produktene som virksomheten tilbyr? | Dette spørsmålet er knyttet til evnen til å opprettholde tilgjengelighet. Relevante aspekter av spørsmålet vil være hvorvidt man har tillit til sentrale leverandører i kjeden, og hvorvidt oversikten over de digitale verdikjedene gir tilstrekkelig informasjon til å fastslå hvem de er. I enkelte sammenhenger vil det også være relevant å vurdere hvorvidt de ligger under norsk jurisdiksjon. |
| **Konfidensialitet** | I hvilken grad kan virksomheten akseptere den risikoen som er knyttet til at andre aktører får tilgang til virksomhetens – muligens krypterte – informasjon? | Dette spørsmålet er knyttet til evnen til å opprettholde konfidensialitet. Relevante aspekter av spørsmålet vil være hvorvidt man har tillit til de som får informasjonen i hende, hvorvidt oversikten over de digitale verdikjedene gir tilstrekkelig informasjon til å fastslå hvem de er, og hvorvidt man stoler på at de ikke kan komme rundt de krypteringsløsningene som er valgt. I enkelte sammenhenger vil det også være relevant å vurdere hvorvidt de ligger under norsk jurisdiksjon. |
| **Integritet** | I hvilken grad kan virksomheten akseptere den risikoen som er knyttet til hvem som er i posisjon til å endre virksomhetens, kundenes eller samfunnets informasjon? | Dette spørsmålet er knyttet til evnen til å opprettholde integritet. Relevante aspekter av spørsmålet vil være hvorvidt man har tillit til de som er i posisjon til å endre informasjon, hvorvidt oversikten over de digitale verdikjedene gir tilstrekkelig informasjon til å fastslå hvem de er, og hvorvidt man stoler på at de ikke kan komme rundt de krypteringsløsningene som er valgt. I enkelte sammenhenger vil det også være relevant å vurdere hvorvidt de ligger under norsk jurisdiksjon. |
| **Insitament** | Har virksomheten tillit til at de som inngår i verdikjeden, arbeider godt nok med å verne om virksomhetens digitale verdier? | Dette spørsmålet er knyttet til hvorvidt man anser at strukturen av SLAer gir alle virksomhetene i verdikjeden tilstrekkelig insitament til god ivaretakelse av de verdiene de er blitt betrodd. |

**TABELL 3.4:** I hvilken grad er den avdekkede risikoen akseptabel?

ufullstendighet, og i en risikoanalyse vil det være viktig å beskrive hva man ikke vet.

Utfallet av risikovurderingen
Vurderingen kan gi ulike utfall:

- Virksomheten kan konkludere med at den foreliggende risikoen er akseptabel.
- Virksomheten kan konkludere med at selv om risikoen i utgangspunktet er uakseptabel, foreligger det ikke realistiske muligheter til å redusere den.
- Virksomheten kan iverksette ytterligere analyser for å forstå risikoen bedre og/eller utforske andre muligheter for risikoreduksjon.
- Virksomheten kan iverksette tiltak for å redusere risikoen til et (mer) akseptabelt nivå.

Det er viktig å være klar over det også for digitale verdikjeder vil være sårbarheter som fremstår som lite tilfredsstillende, men som virksomheten i realiteten ikke har annet valg enn å akseptere. Aksept av restrisiko bør imidlertid være eksplisitt. Det vil si at sårbarhetene bør identifiseres og dokumenteres, og at virksomheten har et avklart forhold til hvorfor risikoen som knytter seg til dem, må aksepteres.

Hvilke tiltak skal iverksettes?
Når virksomheten har kommet til dette punktet i risikostyringsprosessen, må det besluttes hvilke tiltak som skal iverksettes. Deretter må disse implementeres og følges opp. Tabell 3.5 under beskriver tiltakstyper som bør vurderes avhengig av hvilke sårbarheter som er avdekket.

Risikostyring i digitale verdikjeder er en kontinuerlig prosess, hvor de ulike trinnene må repeteres med faste mellomrom eller ved behov. Virksomheten må vurdere i hvilken grad det er behov for rutiner for oppfølging av underleverandørene og eventuelt deres underleverandører for å sikre at den oversikten virksomheten har over verdikjeden er oppdatert og korrekt. Alle tiltak må evalueres for å sikre at ønsket effekt er oppnådd.

| Vurderingselementer | Spørsmål | Aktuelle virkemidler |
|---|---|---|
| **Mangelfull oversikt** | Hvordan håndtere mangelfull oversikt over verdikjeder? | Aktuelle virkemidler her kan være endring av leverandører til noen som tilbyr en bedre oversikt over verdikjedene, eller reforhandling av kontrakter slik at de leverandørene man allerede har gir mer tilfredsstillende informasjon. |
| **Sårbarhet knyttet til tilgjengelighet** | Hvordan håndtere en utilfredsstillende situasjon knyttet til verdikjedens leveringsdyktighet? | Aktuelle virkemidler her kan være å etablere redundante løsninger og/eller stille større krav til robusthet i ikke-redundant løsning |
| **Sårbarhet knyttet til konfidensialitet, og/eller integritet (som også kan påvirke tilgjengelighet)** | Hvordan håndtere en utilfredsstillende situasjon knyttet til hvem som kan påvirke konfidensialitet og/eller integritet? | Aktuelle virkemidler her kan være krypteringsløsninger som bedrer konfidensialitet og integritet. Dersom verdikjeden må endres, vil man måtte skifte ut egne leverandører, eller forsøke å få til endringer lenger ned i kjeden gjennom endrede kontrakter med egne leverandører. |
| **Manglende tillit** | Hvordan håndtere manglende tillit til at leverandørene og/eller underleverandørene i verdikjeden arbeider godt nok med å sikre virksomhetens verdier? | Aktuelle virkemidler her kan være kontraktsfestede tilsynsregimer som gir innsikt i underleverandørenes arbeid med sikkerhet. |

**TABELL 3.5:** Hvilke tiltak skal iverksettes?

KAPITTEL

# 04

# Governance – risikostyring på samfunnsnivå

# 4.1 GOVERNANCE-UTFORDRINGER

Myndighetenes interesse på dette området er primært knyttet til sikkerheten i digitale verdikjeder som har stor betydning for befolkningen og samfunnet. De digitale verdikjedenes kompleksitet, flyktighet og transnasjonale karakter, samt momentan propagering ved svikt eller andre feil i slike kjeder, gjør at styring av risiko i slike kjeder er krevende både på virksomhets- og myndighetsnivå.

Staten kan i begrenset grad styre sikkerheten i de digitale verdikjedene direkte. Trolig er det ingen av disse tjenestene som kan operere uavhengig av leverandører og underleverandører i privat sektor, noen av dem også i utlandet. Virkemidler staten rår over er med andre ord ikke tilstrekkelige for å styre sikkerheten i digitale verdikjeder av kritisk betydning for samfunnet fullt ut. Derfor må ulike typer virkemidler brukes i kombinasjon for å påvirke sikkerheten på best mulig måte.

En rekke tiltak er iverksatt fra statens side uten at disse følger av en samlet plan. Virkemidlene har dels form av reguleringer og har dels et mykere tilsnitt. De digitale verdikjedenes transnasjonale karakter medfører særlige utfordringer. Internasjonalt samarbeid er derfor særlig viktig på dette området, noe som blant annet reflekteres i "Internasjonal cyberstrategi for Norge".[9]

# 4.2 VIRKEMIDLER FOR GOVERNANCE

I et governance-perspektiv kan man skille mellom "harde" og "myke" virkemidler. Hard governance utgjøres av tiltak som springer ut fra offentlige myndigheter og/eller som kan sanksjoneres av myndighetene ved avvik. Myk governance utgjøres av bransjers og bedrifters valgte atferd samt selvregulerende tiltak blant aktørene i verdikjeden uten noen sanksjonerende myndighet knyttet til tiltakene. Myndighetene kan påvirke denne atferden gjennom tilrettelegging, informasjon og ulike offentlig-private samarbeidstiltak.

## 4.2.1 HARD GOVERNANCE

Ulike rettsregler definerer plikter og rettigheter for virksomheter, myndigheter og enkeltpersoner i digitale verdikjeder. Noen er sektorspesifikke og nasjonale, som for eksempel finansavtaleloven for finanssektoren eller energiloven for energiforsyningen.

Andre særlig relevante nasjonale regelsett er:

- Strafferettslige regler (straffeloven)
- Kontraktuelle regler som regulerer plikter og rettigheter blant annet mellom parter i et avtaleforhold, for eksempel i en leveransekjede
- Regelsett som har statssikkerhet og samfunnssikkerhet som formål og som særskilt retter seg mot sårbarheter i samfunnskritiske funksjoner, herunder
  - sikkerhetsloven med forskrifter (se punkt 6.2)
  - utkast til IKT sikkerhetslov (se punkt 6.3)
  - oppfølging av kritiske samfunnsfunksjoner med utgangspunkt i samfunnssikkerhetsinstruksen og som bygger på "KIKS-rammeverket", utviklet av DSB og forankret i to rapporter fra hhv. 2012 og 2016 (se punkt 6.4)
- Sektorlovgivning som regulerer samfunnskritiske tjenester

Andre rettsregler er internasjonale, både sektorielle og generelle, gjerne forankret i ulike internasjonale organer og organisasjoner. Folkeretten gjelder i utgangspunktet også det digitale rommet. Det er imidlertid behov for internasjonal dialog om hvordan folkeretten kommer til anvendelse i cyberdomenet. EU-direktiver og andre EU-regler som er inkorporert i norsk rett er av stor betydning for Norge. For datasikkerhet er spesielt konvensjonen om datakriminalitet forankret i Europarådet

[9] Utenriksdepartementet (2017).

(Budapestkonvensjonen)[10] viktig. Det er i dag ingen FN-konvensjoner eller globale avtaler som særskilt regulerer staters bruk av det digitale rom.

### 4.2.2 MYK GOVERNANCE

Innovasjon og utvikling av digitale tjenester drives i stor grad frem av kommersielle aktører. Myk governance dreier seg om bransjers og virksomheters valgte atferd, samt selvregulerende tiltak blant aktørene i verdikjeden uten sanksjonerende myndighet knyttet til tiltakene. Myndighetenes påvirkning av atferden skjer derfor med andre virkemidler.

Eksempelvis definerer NSMs grunnprinsipper for IKT-sikkerhet et sett med prinsipper og underliggende tiltak for å beskytte informasjonssystemer (maskinvare, programvare og tilknyttet infrastruktur), data og tjenester mot uautorisert tilgang, skade eller misbruk. Grunnprinsippene har en sektorovergripende tilnærming og er et supplement til eksisterende nasjonale og internasjonale regelverk, standarder og rammeverk innen IKT-sikkerhet. De understreker betydningen av å kartlegge leveranser og tilhørende verdikjeder, men det gis ingen nærmere beskrivelser av hvordan dette bør gjøres.

Grunnprinsippene bygger på blant annet standardserien ISO/IEC 27000 om informasjonssikkerhet, som ofte legges til grunn for arbeid med digital sikkerhet. Det internasjonale arbeidet med å utvikle standarder som uttrykker beste praksis på tvers av nasjonale grenser, er av stor betydning på IKT-sikkerhetsområdet. ISO (the International Organization for Standardization) spiller en viktig rolle i denne sammenheng. ISO/IEC 27000-serien inneholder en rekke standarder knyttet til ledelsessystemer for informasjonssikkerhet (ISMS – Information Security Management Systems). [11]

En særlig relevant standard er ISO/IEC 27036 *Information Security for Supplier Relationships*. Standarden omhandler evaluering og håndtering av informasjonssikkerhetsrisiko som er knyttet til innkjøp av varer og tjenester fra en enkelt leverandør.[12] Standarden omhandler relasjoner mellom en kunde og en leverandør, og den beskriver prosesser for anbudsrunder, kontraktsinngåelser, og kontraktselementenes livsløp, inkludert en utviklingsfase dersom systemutvikling er en del av leveransen.[13]

Det finnes også en rekke amerikanske NIST[14]-standarder som blant annet fremholder tillit som en viktig dimensjon ved risikostyringen.[15] Etablering og vedlikehold av tillit mellom aktører i en verdikjede kan utgjøre et viktig "mykt" governance-tiltak, eventuelt kombinert med etablering av klare regler for konsekvenser ved brudd på tillit. Tiltak for å etablere tillit kan for eksempel skje gjennom validering, troverdig tredjepartsvurdering eller sertifisering.[16]

Standardarbeid foregår uten formell involvering av statlige myndigheter. Myndighetene kan likevel delta på lik linje med representanter fra andre fagmiljøer og bør ha en bevisst holdning til hvordan standardisering nasjonalt og internasjonalt kan bidra til styrket sikkerhet i digitale verdikjeder, og hvordan myndighetene kan bidra til dette. Standardene kan også benyttes til å understøtte reguleringstiltak og andre former for "hard" governance.

Myndighetene kan også ha en viktig rolle i å fremme beste praksis på andre måter:

[10] Konvensjon om datakriminalitet – ETS nr. 185.
[11] Norsk Standard (2017).

[12] Andre relevante ISO-standarder i 27000-serien er ISO/IEC 27000 *Information security management systems – Overview and vocabulary, ISO/IEC 27005 Information security risk management, ISO/IEC 27010 Information security management for inter-sector and inter-organizational communications og ISO/IEC 27014 Governance of information security*
[13] Denne standarden har klare berøringspunkter med den modellen som er presentert i kapittel 4, og som har som formål å skaffe oversikt over og styre risiko i digitale verdikjeder. Spesielt vil den delen av modellen vår som heter "Omfang og kontekst – identifisere behov for kartlegging av digitale verdikjeder" bli vesentlig lettere å gjennomføre dersom man har implementert prosesser spesifisert i ISO/IEC 27036 i virksomheten. Videre kan denne standarden inngå som et element i verktøykassen for governance på samfunnsnivå. Prosessene spesifisert i ISO/IEC 27036 gir imidlertid ingen støtte for oversikt over digitale verdikjeder lenger ned enn til leverandørleddet.
[14] National Institute of Standards and Technology (NIST).
[15] Blant de mest relevante standardene er: NIST Special Publication 800-39 (2011): *NS-ISO 31000:2018 Risikostyring – Retningslinjer*Managing Information Security Risk, NIST Special Publication 800-30 (2012): Guide for Conducting Risk Assessment, NIST.SP.800-161 (2015): *Supply Chain Risk Management Practices for Federal Information Systems and Organizations* og NIST.CSWP.04162018 (2018): *Framework for Improving Critical Infrastructure Cybersecurity*.
[16] NIST Special Publication 800-39 (2011): *Managing Information Security Risk*, s. G-1.

- Arbeid for å styrke bransjekultur. Uformelle normer om hvordan kjedeaktivitetene skal utføres både teknologisk og forretningsmessig.
- Etablering av allmenne forventninger til digital sikkerhet som kan fremmes overfor leverandører i kjeden.
- Utarbeide forslag til kravspesifisering knyttet til digital sikkerhet i leverandørkontrakter.
- Videreformidle erfaringer og beste praksis fra ulike internasjonale fora.
- Styrket digital sikkerhet er både i myndighetenes og private virksomheters interesse og er et område som må utvikles gjennom et utstrakt offentlig-privat samarbeid.

# 4.3 FORSVARLIG GOVERNANCE AV DIGITALE VERDIKJEDER

Myndighetene har et særlig ansvar for sikkerheten i grunnleggende nasjonale funksjoner og andre kritiske samfunnsfunksjoner. Dette forutsetter oversikt over og kunnskap om risiko og sårbarhet i digitale verdikjeder som slike funksjoner er avhengige av. I dette inngår også forståelse for teknologiske utviklingstrekk som vil kunne ha betydning for utviklingen i sårbarhetsbildet.

En konseptuell tilnærming til arbeidet med å tydeliggjøre rammene for god governance kan være å kombinere ulike fagperspektiver med ulike former for myk og hard governance. En slik tilnærming er vist i tabell 4.1 under:

Ut fra dette oppsettet er det mulig å definere hvilke harde og myke handlingsnormer de ulike ansvars-posisjonene kan implementere. Det kan være aktuelt å gjøre dette for:

- departementer, både hovedansvarlige[17] og andre
- direktorater og fagetater som forvalter leveranser av kritiske samfunnsfunksjoner gjennom bruk av, eller ved hjelp av, digitale verdikjeder
- sluttleverandører av digitale tjenester til norske kunder
- avtaleparter i kjeden

Slike handlingsnormer sammen med imple-menterende tiltak vil kunne bidra til oversikt og risikostyring av digitale verdikjeder på samfunnsnivå.

| | | |
|---|---|---|
| **Fagperspektiv** | Hard governance | Myk governance |
| **Teknologisk struktur** | Teknologiske krav som er sanksjonert gjennom avtaler og myndighetskrav | Nasjonale og internasjonale fagstandarder<br>Gjensidig faglig forståelse av god teknologisk praksis |
| **Juridisk og institusjonell struktur** | Lover og forskrifter som regulerer aktørenes plikter og legger premisser for avtaleinngåelser<br>Konstituerende styring fra myndigheter som definerer organisatoriske og politisk ansvar<br>Tilsyn etter lov eller forskrift | Juridiske anbefalinger som ikke sanksjoneres<br>Evalueringer, brukerundersøkelser og forskningsaktiviteter<br>Offentlig oppmerksomhet om hendelser<br>Standardisering, akkreditering og sertifisering<br>Internasjonalt diplomati |
| **Økonomi- og tjenestestruktur** | Krav fra virksomhetseier om bærekraftig og forsvarlig forretningsdriv<br>Driftsbeslutninger i kjeden<br>Beredskap og utvikling av redundante tjenester | Tillitsskapende tiltak mellom aktørene<br>Frivillig koordinering i kjeden<br>Markedstilpasninger som respons på svikt |

**TABELL 4.2:** Eksempler på governanceformer

[17] Jf. Justis- og beredskapsdepartementet (2017).

KAPITTEL

# 05

# Anbefalinger

Arbeidsgruppens anbefalinger er rettet til Justis- og beredskapsdepartementet. Gruppens overordnede anbefaling er at departementet bør se til at den modellen som beskrives i rapportens kapittel 4 inngår i og støtter opp under arbeidet med risikostyring i digitale verdikjeder i private og offentlige virksomheter.

I tillegg bør Justis- og beredskapsdepartementet se modellen i sammenheng med andre aktuelle tiltak for å etablere en helhetlig tilnærming til risikostyring av digitale verdikjeder på samfunnsnivå.

# 5.1 UTARBEIDE EN ANBEFALING SOM UNDERSTØTTER NSMs GRUNNPRINSIPPER FOR IKT-SIKKERHET

NSM har i oppdrag å utforme et felles, nasjonalt rammeverk for sikring av IKT-systemer, og etatens grunnprinsipper for IKT-sikkerhet utgjør et basisdokument i denne sammenheng.[18] Grunnprinsippene er utarbeidet for å dekke et bredt spekter av virksomheter, både med hensyn til størrelse og bransje. I motsetning til andre rammeverk som kan ha betydning for risikostyring i digitale verdikjeder, er grunnprinsippene universelle i sin tilnærming – i den forstand at de skal kunne legges til grunn av alle virksomheter.

Grunnprinsippene er det nærmeste man kommer et generelt normgrunnlag for det forebyggende arbeidet med IKT-sikkerhet i Norge, og dokumentet er nær knyttet til sentrale internasjonale standarder og rammeverk. Formålet med grunnprinsippene er "å hjelpe virksomheter å velge sikringstiltak, og gi regelverksforvaltere et rammeverk de kan peke til i sin kravstilling og veiledning".[19]

Grunnprinsippene beskriver *hva* en virksomhet bør gjøre for å sikre et IKT-system. De beskriver også *hvorfor* det bør gjøres, men ikke *hvordan*. I dokumentet pekes det videre på at prinsippene bør brukes som en del av virksomhetsstyringen og gi retning for implementasjons- og driftsnivået i en virksomhet. NSM har utgitt et sett med anbefalinger som understøtter grunnprinsippene.

I siste utgave av dokumentet er det definert 23 grunnprinsipper, hvor det første er at virksomheten må kartlegge leveranser og verdikjeder. Grunnprinsippene inneholder imidlertid ingen definisjon av verdikjeder og ingen omtale av spesielle problemstillinger knyttet til digitale verdikjeder eller utfordringer knyttet til kartlegging av slike.

Arbeidsgruppen foreslår i kapittel 4 en modell for risikostyring i digitale verdikjeder. Modellen er generisk i den forstand at det skal kunne benyttes både i offentlig og privat sektor, i store og små virksomheter. Den er utformet med tanke på at den skal kunne inngå som ledd i statlig regulering eller implementeres frivillig, og den inneholder elementer som allerede omtales i NSMs grunnprinsipper. Det er på denne bakgrunn naturlig at modellen for risikostyring av digitale verdikjeder inngår som del av NSMs anbefalinger knyttet til etatens grunnprinsipper for IKT-sikkerhet.

Modellen bør beskrives som et verktøy for kartlegging og risikostyring, men vil i tillegg ha en normativ funksjon. Den bør utformes slik at den kan brukes både for å imøtekomme krav fra myndigheter og kunder og ut fra virksomhetens egeninteresse.

*Arbeidsgruppen anbefaler:*

- *Problemstillinger og utfordringer knyttet til sikkerhet i digitale verdikjeder bør utdypes i NSMs grunnprinsipper for IKT-sikkerhet.*
- *NSM bør utgi anbefaling for risikostyring i digitale verdikjeder som en operasjonalisering av NSMs grunnprinsipper for IKT-sikkerhet. Utgangspunktet er modellen som presenteres i kapittel 4 i denne rapporten.*
- *NSM bør videreutvikle den anbefalte modellen for risikostyring av digitale verdikjeder sammen med relevante aktører og i lys av lignende arbeid som foregår internasjonalt.*

[18] NSM (2018).
[19] Ibid.

## 5.2 TA INN BEHOVET FOR SIKRING AV DIGITALE VERDIKJEDER I SIKKERHETSLOVEN MED FORSKRIFTER OG VEILEDERE

Ny sikkerhetslov med forskrifter trådde i kraft 1. januar 2019. Det er ennå for tidlig å danne seg en oppfatning av i hvilken grad det nye regelverket vil bidra til å styrke sikkerheten i digitale verdikjeder.

Virksomheter underlagt loven skal kartlegge andre virksomheter som de i *vesentlig* eller *avgjørende* grad er avhengig av for å ivareta grunnleggende nasjonale funksjoner. Virksomhetenes kartleggingsarbeid skal basere seg på en risikovurdering. Der en virksomhet avdekker at det foreligger *vesentlige* eller *avgjørende* avhengigheter som innvirker på dens evne til å ivareta en grunnleggende nasjonal funksjon, skal den vurdere mulige tiltak.

Relevante tiltak kan være å endre verdikjeden slik at sårbarheten som følger av den identifiserte avhengigheten reduseres. Et annet alternativ er å melde avhengigheten til eget sektordepartement. Dersom en virksomhet melder inn en *avgjørende avhengighet* av en annen virksomhet, skal denne virksomheten underlegges loven etter enkeltvedtak. (Virksomheter som utgjør en *vesentlig* avhengighet skal det kun føres oversikt over i departementet.)

Kartleggingen av verdikjeden kan fortsette ved at de virksomheter som blir underlagt loven som følge av at det er avdekket avhengighetsforhold til en annen virksomhet, igjen kartlegger egne avhengigheter og melder inn *vesentlige* og *avgjørende* avhengigheter som ikke kan reduseres, til eget sektordepartement.[20]

Arbeidsgruppen oppfatter at det kan være noe uklart om virksomhetene er pålagt selv å ha oversikt lenger enn til første ledd. Slik arbeidsgruppen tolker det, stiller ikke loven eksplisitt krav om at den enkelte virksomhet skal ha oversikt over *hele* sin verdikjede.

Dersom virksomheten oppfatter at den har redundans på et område, vil avhengigheten antagelig også kunne bli definert som *vesentlig* og ikke *avgjørende*, eller kanskje ikke innrapportert i det hele tatt. Dermed kan sårbarheter i form av falsk eller svekket redundans lenger ute i kjeden forbli ukjente og usikrede.

*Arbeidsgruppen anbefaler:*

- *Modellen for risikostyring i digitale verdikjeder bør tas inn i, eller refereres til, i NSMs veiledere til sikkerhetsloven med forskrifter.*
- *Ved en fremtidig evaluering av sikkerhetsloven med forskrifter bør det legges særlig vekt på å vurdere i hvilken grad loven har bidratt til å styrke sikkerhet i digitale verdikjeder.*
- *Ved revisjon av loven og dens forskrifter bør det vurderes å tydeliggjøre at virksomheter som er underlagt loven selv skal ha oversikt over egne digitale verdikjeder av betydning for grunnleggende nasjonale funksjoner, og at denne oversikten skal gjøres tilgjengelig for sikkerhetsmyndigheten.*

## 5.3 TA INN BEHOVET FOR SIKRING AV DIGITALE VERDIKJEDER I FORSKRIFT TIL NY NIS-LOV SAMT I EKSISTERENDE SEKTORREGELVERK

Et utkast til lov om sikkerhet i nettverk og informasjonssystemer vurderes for tiden i JD. Loven skal implementere EUs NIS-direktiv i norsk rett. Lovens virkeområde er i utgangspunktet definert gjennom en opplisting av virksomhetstyper i et vedlegg til direktivet. I høringsrunden på utkastet kom det flere innspill som gikk på å utvide lovens virkeområde til å omfatte flere sektorer. Dette var også en anbefaling i NOU 2018:14 *IKT-sikkerhet i alle*

[20] Prop. 153 L (2016-2017) Lov om nasjonal sikkerhet og Forskrift om virksomheters arbeid med forebyggende sikkerhet (virksomhetsikkerhetsforskriften).

*ledd - Organisering og regulering av nasjonal IKT-sikkerhet.*

NIS-direktivet er i utgangspunktet relativt generelt og overordnet. Det norske utkastet til lov foreslår at tilbydere av samfunnsviktige tjenester skal gjennomføre en risikovurdering av de nettverk og informasjonssystemer som benyttes for å levere tjenesten. Det skal på denne bakgrunn gjennomføres "hensiktsmessige og proporsjonale tekniske og organisatoriske tiltak" for å redusere risikoen.

Om digitale verdikjeder inngår i "de nettverk og informasjonssystemer som benyttes for å levere tjenesten" er et åpent spørsmål. Loven er enda ikke fremmet for Stortinget, og det skal i ettertid også utarbeides forskrifter og veiledninger til den. I den forbindelse bør risikostyring i digitale verdikjeder omtales spesielt.

NIS-loven vil bare gjelde områder som ikke allerede er regulert i eksisterende lovverk og som stiller minst tilsvarende krav til sikkerhet som NIS-loven. En naturlig konsekvens av dette vil være at sikkerhet i digitale verdikjeder også omtales eksplisitt i forskrifter og/eller veiledning til relevant sektor-regelverk. Ekom-området peker seg ut som spesielt viktig i denne sammenheng.

Videre er det nødvendig å vurdere behovet for oppdateringer av virkemiddelapparatet jevnlig, blant annet basert på oppdatert kunnskap om teknologi-utviklingen nasjonalt og internasjonalt. IKT-teknologien har alltid vært preget av en høy endringstakt. Dette er en utfordring for myndig-hetene, da eksisterende lovgivning og reguleringer eldes i høyere tempo på dette området enn på de fleste andre. Også for reguleringer knyttet til digitale verdikjeder vil dette gjøre seg gjeldende. Endrings-takten på de digitale verdikjedene kan øke vesentlig i årene som kommer. Blant annet gjør virtualiserings-teknologien at serverfunksjoner kan flyttes fra ett sted til et annet bare med et tastetrykk, noe som vil kunne føre til gjennomgripende endringer i verdikjeden.

*Arbeidsgruppen anbefaler:*

- *En påpekning av viktigheten av å kartlegge og redusere sårbarheter i digitale verdikjeder bør tas inn i forskriften til ny lov om sikkerhet i nettverk og informasjonssystemer (NIS-direktivet i norsk lov). I veiledning til loven bør det vises til NSMs grunnprinsipper og modell for risikostyring i digitale verdikjeder.*
- *Tilsvarende bør modellen for risikostyring i digitale verdikjeder tas inn i forskrifter og veiledere til relevant sektorlovverk.*

## 5.4 TA INN BEHOVET FOR SIKRING AV DIGITALE VERDIKJEDER VED REVISJON AV KIKS-RAMMEVERKET

DSBs rapport om Samfunnets kritiske funksjoner (KIKS-rammeverket, 2016) er knyttet til Justis- og beredskapsdepartementets samfunns-sikkerhetsinstruks[21] og slik førende for hvilke samfunnsfunksjoner departementene skal legge særlig vekt på å opprettholde uavhengig av hva som måtte inntreffe.

Hensikten med KIKS-rammeverket er å sikre opprettholdelse av samfunnets grunnleggende funksjonsdyktighet. Den første rapporten som ble utarbeidet om disse forholdene i 2012 hadde større oppmerksomhet på hvordan samfunnet måtte arbeide for å lykkes med dette enn rapporten fra 2016.[22] Den sistnevnte rapporten består i prinsippet av en gjennomgang og konkretisering av hvilke funksjoner og leveranser som departementene må legge vekt på å opprettholde.

Justis- og beredskapsdepartementet utga i september 2019 en veileder for arbeidet knyttet til samfunns-sikkerhetsinstruksen. Verken veilederen eller KIKS-rammeverket inneholder noen beskrivelse av problemstillinger knyttet til digitale eller andre verdikjeder.

[21] Justis- og beredskapsdepartementet (2017).)).
[22] Direktoratet for samfunnssikkerhet og beredskap (2012) og (2016).

Selv om KIKS-rammeverket primært er utviklet for å målrette samfunnssikkerhetsarbeidet i departementene, brukes det også i mange andre sammenhenger og av andre aktører. Rammeverket har bidratt til å styrke oppmerksomheten på virksomheters funksjonsdyktighet og leveringsevne og risikostyringen innenfor kritiske samfunnsfunksjoner.

*Arbeidsgruppen anbefaler:*

- *Ved revisjon av KIKS-rammeverket bør det pekes på hvordan departementene (og andre myndighetsaktører) kan arbeide for å kartlegge og redusere sårbarheter. I denne sammenheng bør sårbarheter i digitale verdikjeder omtales spesielt, og det bør henvises til modell for risikostyring i digitale verdikjeder.*

## 5.5 HELHETLIG TILNÆRMING TIL GOVERNANCE AV DIGITALE VERDIKJEDER

Begrepet *governance* er i denne rapporten brukt om risikostyring på samfunnsnivå. Mange digitale tjenester er av stor betydning for nasjonal sikkerhet og for samfunnssikkerheten for øvrig. Kompleksiteten i digitale verdikjeder og kjedenes transnasjonale karakter gjør det krevende å sikre at samfunnets sikkerhetsbehov er ivaretatt. Det er viktig at myndighetene har en helhetlig tilnærming til hvordan virkemidlene staten rår over best kan benyttes i risikostyringen på samfunnsnivå.

Digitale verdikjeder kan betraktes ut fra så vel teknologiske, juridisk og institusjonelle og økonomiske og tjenestemessige fagperspektiver. Disse strukturene påvirkes i dag med ulike virkemidler, både "harde" og "myke", fra statens side, uten at dette nødvendigvis springer ut av en samlet, planmessig eller konseptuell tilnærming.

Å beskrive handlingsnormer knyttet til de ulike fagperspektivene, jf. tabell i kapittel 5.3, vil bidra til en mer systematisk tilnærming til risikostyring i slike verdikjeder på samfunnsnivå. Anbefalingene i kapittel 6.1 – 6.4 over kan inngå som viktige elementer i et slikt system. Modellen for risikostyring i digitale verdikjeder som presenteres i kapittel 4 kan være et sentralt virkemiddel for å gi myndighetene oversikt over digitale verdikjeder. Den kan knyttes opp mot "hard governance" i form av reguleringer som sikkerhetsloven, en ny lov som implementerer EUs NIS-direktiv, sektorlovgivning og KIKS-rammeverket gjennom forskriftsverk og veiledere.

Modellen vil også kunne være et "mykt" tiltak gjennom å innarbeides som "beste praksis", knyttes opp mot NSMs grunnprinsipper for IKT-sikkerhet, videreutvikles som en nasjonal og eventuelt internasjonal standard eller for eksempel presenteres på ulike konferanser og seminarer.

En systematisk og strukturell tilnærming til governance vil kunne bidra til en god forvaltning av den samlede kunnskapen som myndighetene vil få gjennom de ulike type tiltakene. Å få oversikt over risiko og sårbarhet i de digitale verdikjedene er ikke et mål i seg selv, men et delmål i arbeidet med god risikostyring. Kunnskapen og oversikten man skaffer seg må aktivt benyttes i det videre arbeidet med å styrke arbeidet med IKT-sikkerhet og redusere sårbarhet i digitale verdikjeder.

Risikostyring i digitale verdikjeder må for øvrig ses i en internasjonal kontekst. Utviklingen skjer raskt og utfordrer løpende norske myndigheter og norsk næringsliv både strategisk og teknisk. Andre, vesentlig større land enn Norge, utvikler fortløpende strategier, handlingsplaner og konkrete tiltak for å møte utviklingen med nye sikkerhetstiltak. I arbeidet med risikostyring i digitale verdikjeder er det derfor av avgjørende betydning å være oppdatert både på den teknologiske utviklingen og utviklingen av sikkerhetstiltak i andre land.[23]

Norge bør ta aktivt del i internasjonalt standardiseringsarbeid og internasjonalt reguleringsarbeid på dette området. Det er likevel arbeidsgruppens oppfatning at Norge har kommet lengre enn svært mange land i arbeidet med sikkerhet i digitale verdikjeder. Vi bør derfor kunne

[23] Utenriksdepartementet (2017) og NSM (2015).

spille en aktiv pådriverrolle i dette arbeidet internasjonalt.

*Arbeidsgruppen anbefaler:*

- *Justis- og beredskapsdepartementet bør utrede nærmere og beslutte hvordan ulike statlige virkemidler skal benyttes for en overordnet samfunnsmessig risikostyring av digitale verdikjeder av stor betydning for befolkningens og samfunnets sikkerhet. Elementer i denne sammenheng kan være:*
  - *Veiledning for å fastsette digitale verdier*
  - *Veiledning for nivåspesifisering av akseptert digital sårbarhet*
  - *Sårbarhets- og verdivurderinger ved større avtaleinngåelser*
  - *Forsknings- og utviklingstiltak*
- *Justis- og beredskapsdepartementet, Forsvarsdepartementet, Utenriksdepartementet og øvrige aktuelle sektordepartement bør se til at Norge tar del i internasjonale initiativer for å etablere standarder, samt identifisere og implementere tiltak utviklet internasjonalt som gir mer effektive og sikre digitale verdikjeder.*
- *Regjeringen bør vurdere å utarbeide en strategi for ivaretagelse av sikkerhet i transnasjonale digitale verdikjeder*

# Vedlegg

# DATAGRUNNLAG

## SAMTALER

5. mars 2019: Espen Heiberg, Nasjonal sikkerhetsmyndighet

5. mars 2019: Jon Arne Gisnås, Justis- og beredskapsdepartementet

4. april 2019: Jan Vidar Moen, Forsvarsstaben Plan IKT

4. april 2019: Kjetil Sveen, Forsvarets sikkerhetsavdeling

## REFERANSER


Aven, Røed og Wiencke (2008): *Risikoanalyse*. Universitetsforlaget, Oslo Bøe et. al (2012): *Sikkerhetstenkning før og nå – en litteraturstudie*

Direktoratet for samfunnssikkerhet og beredskap (2012): *Sikkerhet i kritisk infrastruktur og kritiske samfunnsfunksjoner – modell for overordnet risikostyring*

Direktoratet for samfunnssikkerhet og beredskap (2016): *Samfunnets kritiske funksjoner. Hvilken funksjonsevne må samfunnet opprettholde til enhver tid?*

Europaparlaments- og rådsdirektivet (EU) 2016/1148 av 6. juli 2016 om tiltak for å sikre et høyt felles nivå for sikkerhet i nett- og informasjonssystemer i hele Unionen. Uoffisiell oversettelse

Forsvarsdepartementet: Prop. 153 L (2016-2017) *Lov om nasjonal sikkerhet (sikkerhetsloven)*

Forsvarsdepartementet: Prop. 1 S (2017-2018))

ISO/IEC 27000-serien om IKT-sikkerhet

ISO/IEC 27036:2014 *Information Security for Supplier Relationships*

Justis- og beredskapsdepartementet (2015): NOU 2015:13 *Digital sårbarhet – sikkert samfunn*

Justis- og beredskapsdepartementet (2016): Meld. St. 10 (2016-2017). *Risiko i et trygt samfunn. Samfunnssikkerhet*

Justis- og beredskapsdepartementet (2016): Meld. St. 38 (2016-2017) *IKT-sikkerhet. Et felles ansvar*

Justis- og beredskapsdepartementet (2017): *Instruks for departementenes arbeid med samfunnssikkerhet*

Justis- og beredskapsdepartementet (2018): NOU 2018:14 *IKT-sikkerhet i alle ledd — Organisering og regulering av nasjonal IKT-sikkerhet*

Justis- og beredskapsdepartementet (2019): Forskrift om virksomheters arbeid med forebyggende sikkerhet (virksomhetssikkerhetsforskriften)

Konvensjon om datakriminalitet – ETS nr. 185 (Budapestkonvensjonen)

Nasjonal sikkerhetsmyndighet (2015): Sikkerhetsfaglige råd

Nasjonal sikkerhetsmyndighet (2016): Sjekkliste nr 1 (S-01) *Fire effektive tiltak mot dataangrep. Oppdatert 2016-03-03.*

Nasjonal sikkerhetsmyndighet (2018) *Grunnprinsipper for IKT-sikkerhet, versjon 1.1*

National Institute of Standards and Technology (2011): NIST Special Publication 800-39: Managing Information Security Risk, s. G-1

National Institute of Standards and Technology (2012): NIST Special Publication 800-30: *Guide for Conducting Risk Assessment*

National Institute of Standards and Technology (2015): NIST.SP.800-161 (2015): *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*

National Institute of Standards and Technology (2015): NIST.SP.800-161: *Supply Chain Risk*

*Management Practices for Federal Information Systems and Organizations*

National Institute of Standards and Technology (2018): NIST.CSWP.04162018: *Framework for Improving Critical Infrastructure Cybersecurity*

Standard Norge (2018): NS-ISO 31000:2018 *Risikostyring. Retningslinjer*

Standard Norge (2008): NS 5814:2008 *Krav til risikovurdering*

Standard Norge (2014): NS 5832:2014 *Samfunnssikkerhet - Beskyttelse mot tilsiktede uønskede handlinger - Krav til sikringsrisikoanalyse*

Perrow, Charles (1984): *Normal Accidents: Living with High Risk Technologies. Basic Books*

Porter, Michael (1985): *Competitive Advantage. The Free Press. A division of Macmillian, Inc. New York*

Utenriksdepartementet (2017): *Internasjonal cyberstrategi for Norge*

Utkast til lov om sikkerhet i nettverk og informasjonssystemer *(NIS-direktivet i norsk lov)*

Direktoratet for
samfunnssikkerhet
og beredskap

**DSB**
**Rambergveien 9**
**Postboks 2014**
**3103 Tønsberg**

**+47 33 41 25 00**

**postmottak@dsb.no**
**www.dsb.no**

/DSBNorge @dsb_no
dsb_norge dsbnorge

**ISBN 978-82-7768-496-3 (PDF)**
**HR 2422**
**Januar 2020**