

Verdiskaping i AI-æraen

Ferdighetene som kreves og viktigheten av sikker AI-klar infrastruktur



Radar.

Om rapporten

Denne rapporten henvender seg til beslutningstakere og virksomhetsledere innen både privat og offentlig sektor som ønsker å forstå hva som kreves for å muliggjøre en transformativ verdiskaping med AI. Formålet med rapporten er å gi svenske (og norske) virksomheter og beslutningstakere handlingsbar innsikt om neste fase av AI – som grunnlag for strategi, prioriteringer og beslutninger.

Rapporten tar utgangspunkt i sentrale ytre og indre drivkrefter påvirker virksomheters arbeid med AI nå og fremover. Med utgangspunkt i drivkreftene som styrer strategier og prioriteringer, gjøres et dypdykk i dagens situasjon for virksomheters bruk, modenhet og verdiskaping med den nye teknologien. Deretter diskuteres neste æra av AI; hva den innebærer, hvordan den skiller seg fra dagens AI og hvilke krav og behov den vil skape hos virksomheter. Til slutt defineres reisen mot målbildet og hvilke hindringer samt muliggjørere som må vurderes innen dimensjonene mennesker, virksomhet og teknologi. I tillegg bidrar rapporten med en enkel veiledning og konkrete anbefalinger for en mer effektiv og sikker AI-reise.

Rapporten er utarbeidet i et samarbeid mellom Cisco og Radar Group. Grunnlaget for rapporten består av nordiske spesifikke data samt åpne og tilgjengelige data som er analysert sammen med kvalitativ innsikt fra både dybdeintervjuer og rundebordssamtaler. Den kvalitative undersøkelsen er gjennomført med et tjuetalls respondenter i ledende stillinger fra både privat og offentlig sektor. Respondentene ble håndplukket for å representere ulike perspektiver; som teknologi, virksomhetsledelse, politikk, sikkerhet, infrastruktur, samt ulike perspektiver innen offentlig forvaltning.

Rapportens fokus

Rapporten undersøker neste æra av AI, som preges av mer autonome systemer og mer virksomhetsnære anvendelser, og diskuterer hvordan vi er rustet til å møte den. Fokus ligger på de nye mulighetene for verdiskaping og hvilke underliggende kapabiliteter som må styrkes for å lykkes med å realisere dem. Rapportens tyngdepunkt og bidrag er derfor å veilede beslutningstakere i hvordan de skal agere og prioritere for å skape reelle virksomhetsverdier ved hjelp av AI.

For å lykkes med dette trengs et perspektivskifte – fra et teknologidrevet perspektiv der AI legges oppå eksisterende forretningsprosesser og flyter, til et mer innovativt og transformativt perspektiv der virksomheten utfordrer sine eksisterende forretningsprosesser, skaper nye flyter og dermed også nye verdier. Rapporten introduserer dermed to begreper som vil være gjennomgående: forventningsstyrte og nyttestyrte virksomheter.

Forventningsstyrte virksomheter

Forventningsstyrte virksomheter utgjør et bredt spenn, og det er her majoriteten av virksomheter befinner seg i dag. De preges i høyere grad av et teknologidrevet fokus og et utenfra-perspektiv. Arbeidet med AI er basert på en reaktiv forventning om hvilke verdier AI kan skape ved å kun gjennomføre et teknologiskifte eller tillegg. Tydelige bruksområder (use cases) eller formuleringer av hvilke verdier AI skal skape mangler ofte, og arbeidet har en tendens til å være utforskende snarere enn strategisk forankret. Mange forventningsstyrte virksomheter opplever akkurat nå et gap mellom forventning og den reelle verdiskapingen, ettersom de potensielle verdigevinstene som ofte løftes frem i eksterne medier, ennå ikke har blitt realisert som ønsket.

Nyttestyrte virksomheter

En nyttestyrt virksomhet tar i større grad utgangspunkt i sin overordnede strategi og våger i større utstrekning å utfordre eksisterende arbeidsprosesser og flyter ved hjelp av ny AI-teknologi. De har en systematisk arbeidsmåte der strategi, infrastruktur, data, styring, mennesker og kultur balanseres. AI sees på som en av flere komponenter og en muliggjør for reelle virksomhetsbehov. Den tydeligere retningen gjør at den nyttestyrte virksomhetens arbeid med AI ofte er mer effektivt og treffsikkert, noe som gjør at de fanger nye og større verdier og nytteverdier. Nyttestyrte virksomheter med et mer robust grunnlag for arbeidet har dessuten bedre forutsetninger for å fange den eksponentielle verdiutviklingen når vi går inn i neste æra av AI.

Denne rapporten bidrar til å flytte perspektivet fra det forventningsstyrte til det nyttestyrte. Snarere enn å tilskrive AI en egenverdi, sees teknologien som et, om enn svært kraftfullt, verktøy i verktøykassen for å gjennomføre strategier og mål. En positiv sideeffekt av å gjøre denne kulturendringen er at innovasjonsevnen styrkes. Ikke bare for å optimalisere det som allerede finnes, men også for å utforske helt nye muligheter. I tillegg styrkes også produktivitet, effektivitet og lønnsomhet. Faktum er at årets utgave av Cisco AI Readiness Index blant annet viser at nyttestyrte virksomheter har 1,5 ganger høyere sannsynlighet for å hente ut verdi med sine AI-initiativer, noe som vil være avgjørende når vi beveger oss mot neste generasjons AI.

1.5x høyere sannsynlighet for å hente ut
verdi med sine **AI-initiativer²** (faktor)



Inholdsfortegnelse

Faktorer som former dagens AI-reise	7
Ytre faktorer	7
Indre faktorer	11
AI-reisen frem til nå	13
Bruksgrad og modenhet	13
Dagens AI-verdiskapning	14
AI-reisen fram til nå: offentlig og privat sektor i sammenligning	17
Forutsetninger	17
Muligheter og handlingsrom	17
Privat og offentlig sektors unike styrker	19
Målbildet for en AI-drevet fremtid	20
Fra teknologidrevet til strategisk forankret	20
Flyttes til neste side	21
Fra individ til virksomhet	22
Fra innelåsing til kontroll	23
En helt ny verdiskaping	24
Endringsreisen mot målbildet	25
Målbildet styres av virksomhetsbehov	25
Utfordringer og muliggjørere	25
Kapabilitetene som kreves for å lykkes med reisen	39
Veiledning for en verdiskapende AI-reise	39
Fra teori til praksis: Cisco's rolle i AI-reisen	45
Konkrete sluttanbefalinger til beslutningstakere	48
Sluttord	49
Referanseliste	50

Faktorer som former dagens AI-reise

For å forstå dagens situasjon, målbildet og endringsreisen som venter, kreves innsikt i drivkreftene som former utviklingen. AI kan ikke ses som et isolert område, men påvirkes av et sett ytre og indre faktorer. Derfor må AI plasseres i en bredere kontekst for å tydeliggjøre utviklingens retning og de forutsetningene og behovene som preger arbeidet fremover.

Ytre faktorer

Det har sjelden vært så komplekst å navigere virksomheten i det rådende omverdensbildet. Geopolitiske skifter, et regulatorisk landskap i endring og et stadig mer utfordrende cybersikkerhetslandskap har lenge vært sentrale omverdensfaktorer. Det som gjør situasjonen annerledes i dag, er at AI tydelig endrer dynamikken innen samtlige tre områder. AI påvirker hvordan problemstillingene oppstår, deres karakter, hvilke risikoer og muligheter de innebærer, og hvordan virksomheter må tenke strategisk fremover.

GEOPOLITIKK OG SUVERENITET

IT og teknologi er sentrale arenaer i dagens geopolitiske maktkamp, og mye av dynamikken kretser rundt kappløpet innen AI. Å lede utviklingen og bruken av AI har blitt en sentral prioritet for aktører som ønsker å styrke sin politiske og økonomiske stilling. Ofte handler denne diskusjonen om USA og Kina, men Europa står i stadig større grad for en egen retning.

Europas AI-strategi er sentrert rundt fortreffelighet og tillit. Ambisjonen om teknologisk konkurransekraft kombineres med et sterkt fokus på transparens, sikkerhet og integritet, noe som også gjenspeiles i unionens regulatoriske rammeverk. Enkelte regelverk, som AI-forordningen og GDPR, styrker individets integritet og sikkerhet ved å regulere hvordan data og AI kan brukes. Andre, som forordningen om digitale markeder (DMA), har som

mål å styrke den digitale autonomien ved å fokusere på konkurranse og antitrust-spørsmål innen den digitale sektoren.

I den senere tid har suverenitetsdiskusjonen gått over til å handle mer om integritets- og beskyttelsesorientert datasuverenitet, der fokus ligger på organisasjonenes egne interesser. I dag er det en økt interesse for å styrke egen evne og sikre kontroll og råderett over egen digital virksomhet og beslutninger. Denne utviklingen drives delvis av det økte fokuset på geopolitisk suverenitet, og delvis av endrede relasjoner mellom USA, Kina og Europa. Både AI og suverenitet blir stressfaktorer på allerede kjente bekymringer og driver endrede prioriteringer og strategier for å komme i kapp og styrke både konkurransekraft og motstandskraft.

REGULATORISK LANDSKAP

Gitt EUs strategi for digital suverenitet, finnes det fra før flere omfattende regelverk som styrer den digitale sektoren, men AI transformerer dette landskapet i bunn og grunn. Siden teknologien bygger på data, påvirkes den av hvordan informasjon skapes og distribueres, samt endringer i arbeidsmåter og beslutningsprosesser knyttet til data. Dette innebærer at AI berører mange av de eksisterende reguleringene og deres anvendelser.

I denne sammenhengen fortjener imidlertid AI-forordningen spesiell oppmerksomhet. Forordningen er et av EUs nyeste digitalpolitiske regelverk og er også verdens første helhetlige lovgivning rettet direkte mot AI, til forskjell fra tidligere rammeverk som bare har berørt teknologien indirekte. Paradoksalt nok er det først og fremst mangelen på oppmerksomhet rundt AI-forordningens gjennomslag som gjør den mest bemerkelsesverdig. Dette skal imidlertid ikke tolkes som at beslutningstakere mangler interesse for regulatoriske rammeverk, da:

48% av IT-beslutningstakere ser manglende **regulatorisk etterlevelse og oppfølging** som en potensiell risiko ved AI-bruk, noe som er en økning på 13 prosentpoeng siden 2024⁸.

Hva som inkluderes i begrepet «regulatoriske rammeverk» kan variere mellom virksomheter og avhenger av hvilke regelverk de omfattes av. Derimot fremgår det i rapportens undersøkelse at AI-forordningen ikke gis høy prioritet, og at mange opplever at de ikke har rukket å fordype seg i hva den innebærer ennå. I dag preges arbeidet med AI først og fremst av tekniske og operative overveielser snarere enn regulatoriske. Fokus ligger på å utforske og teste teknologien, samt å finne måter å implementere den i virksomheten på. Det finnes usikkerhet rundt hvordan AI-forordningen er relevant for den egne virksomheten, og rammeverket ses verken som en direkte støtte eller en trussel, og vurderes ikke som spesielt presserende på nåværende tidspunkt.

Blant virksomhetene som har tatt stilling til AI-forordningen, finnes det en del bekymring rundt dens omfang, samt at forordningen skal ha en for bred definisjon av høyrisikosystemer, noe som risikerer å begrense handlingsrommet for virksomheter. I tillegg fremkommer det en mer overordnet bekymring for at regulatoriske rammeverk reduseres til en ren etterlevelsesevne, der fokus havner på å formelt oppfylle kravene snarere enn å arbeide i tråd med deres formål og intensjon. Et nærliggende spørsmål knyttet til dette berører ansvarsfordeling, der de nåværende mekanismene ikke vil være tilstrekkelige for særskilte virksomheter eller anvendelser, og at AI-forordningen da risikerer å bli brukt som en unnskyldning for feil eller mangelfulle beslutninger. Frykten ligger i at AI brukes som en syndebykk, der ansvar kan skyves over på teknologien når noe går galt. I denne sammenhengen kan AI-forordningen fungere som et legitimt grunnlag for slike beslutninger, ved at virksomheter kan henvise til at de har agert i samsvar med regelverket.

Fordypning: AI-forordningen

Formålet med AI-forordningen er å innføre felles spilleregler innen EU for hvordan AI utvikles, slippes på markedet, tas i bruk og brukes. Forordningen skal sikre at AI-systemene er menneskesentrerte, sikre, respekterer grunnleggende rettigheter og samtidig fremmer innovasjon og investeringer. Den skal også garantere fri bevegelse for AI-baserte varer og tjenester innen unionen. AI-forordningen gjelder alle som utvikler, tilbyr, importerer, distribuerer eller bruker AI-systemer (også tredjeparter utenfor EU).

AI-forordningen bygger på en risikobasert modell der visse bruksområder er forbudt, mens andre tillates med krav. Tyngdepunktet

ligger på AI-systemer med høy risiko – det vil si systemer som kan medføre betydelig skade for helse, sikkerhet eller grunnleggende rettigheter, men omfatter også forbud og regler for AI-modeller for generelle formål. Høyrisikosystemer må oppfylle en pakke med grunnkrav gjennom hele livssyklusen – risikostyring og tester, kvalitetsstyringssystem, kvalitetskontrollerte data, teknisk dokumentasjon, automatisk logging, tydelig informasjon til brukere, menneskelig kontroll samt krav til nøyaktighet, robusthet og cybersikkerhet. I tillegg gjelder særskilte transparenskrav: når mennesker samhandler med AI skal det fremgå, og AI-generert innhold skal merkes.

CYBERSIKKERHETSSITUASJONEN

I dag står virksomheter overfor en utfordrende cybersikkerhetssituasjon, og trusselbildet har blitt transformert og mer komplekst og vanskelig å håndtere som følge av AI. Teknologien gjør det mulig å automatisere angrep, generere overbevisende kommunikasjon for nettfiske (phishing) og gjennomføre avanserte kampanjer med sosial manipulering. Denne utviklingen blir mer merkbar i takt med at AI-modellene blir kraftigere, mer lett tilgjengelige og brukervennlige, noe som gjør det mulig for flere aktører å utnytte dem til skadelige formål. Cyberangrep og påvirkning brukes i dag som virkemidler i den geopolitiske maktkampen, og høy cybersikkerhet blir en viktig nøkkel for å oppnå suverenitet, etterleve lovkrav og beskytte virksomheten mot risiko. Dette setter AI-kappløpet på spissen. Samtidig som regelverk som AI-forordningen oppfordrer til en ansvarlig og kontrollert AI-implementering, driver trusselbildet et behov for å raskt øke AI-modenheten for ikke å havne bak trusselaktørene. AI blir et nødvendig verktøy i kampen mot AI-baserte trusler.

**Nyttestyrte
virksomheter**
har

2x

høyere bevissthet om AI-spesifikke trusler
sammenlignet med markedsgjennomsnittet².

55%

ser risikoer for virksomhetens cybersikkerhet
ved bruk av AI⁸.

Indre faktorer

De ytre faktorene som påvirker AI-landskapet får tydelige konsekvenser og gjennomslag i virksomhetene. Inntoget av ny teknologi skjer i en akselererende fart og endrer forutsetningene fra grunnen av. Nesten en femtedel av svenske IT-beslutningstakere opplever ny teknologi, som AI eller kvanteteknologi, som mest disruptivt for virksomheten i 2026⁸.

AI har samtidig gått fra å være et spørsmål for IT-beslutningstakere til i stadig større grad å bli noe som hele virksomheten må forholde seg til. Spørsmålet gjennomsyrrer i dag organisasjonen både direkte og indirekte, og påvirker strategier, prioriteringer og utfordringer. Samtidig kjemper mange med å henge med og forstå hva den nye teknologien innebærer for egen virksomhet.

PRIORITERINGER OG UTFORDRINGER

Blant svenske IT-beslutningstakers fremste strategiske prioriteringer og utfordringer frem mot 2026 kan nesten samtlige kobles til AI på ulike måter. Fra topplasseringen i fjor har automatisering gått forbi strategisk sikkerhet på prioriteringslisten. I tillegg klatrer flere områder innen datahåndtering opp som både utfordrende og prioriterte, noe som tyder på en økende innsikt i hvordan disse områdene henger sammen. Datakvalitet, styring og databeskyttelse er alle kritiske komponenter for å lykkes med så vel cybersikkerhetsarbeidet som digitalisering og automatisering. Samtidig gjenspeiler det faktum at AI-relaterte områder finnes både som prioriteringer og utfordringer at fremgang kan være tøft å oppnå, og at takt og modenhet kan være ujevn.

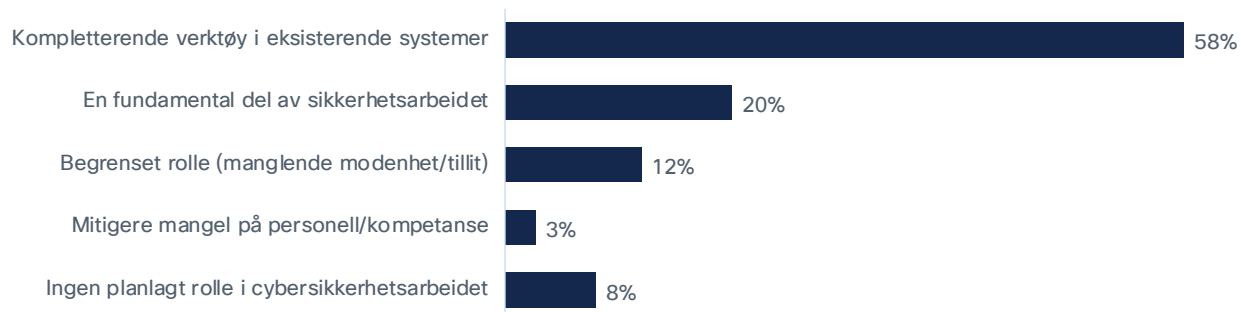
IT-strategiske prioriteringer ⁸	IT-strategiske utfordringer ⁸
63% Automatisering – effektivitet og produktivitet	45% Sikkerhet – strategi og etterlevelse
55% Sikkerhet – strategi og etterlevelse	39% Digitalisering – virksomhets- og forretningsmodeller
54% Datahåndtering – kvalitet og styring	35% Datahåndtering – kvalitet og styring
46% Digitalisering – virksomhets- og forretningsmodeller	30% Styring – redusere IT-kostnader
39% Applikasjoner – forvaltning av eksisterende	27% Datahåndtering – kvalitet og styring

AI I CYBERSIKKERHETSSTRATEGIER

Cybersikkerhet er et av de viktigste fokusområdene for virksomheter, og AI må tas i betraktning i cybersikkerhetsstrategier. Praktiske bruksområder for AI innen cybersikkerhet inkluderer systemer for å identifisere avvik, automatisert prioritering (triage) av alarmer og plattformer for trusseletterretning som samler store datamengder og finner korrelasjoner ingen mennesker kan oppdage i sanntid. Til tross for mulighetene AI kan tilføre sikkerhetsarbeidet, bruker de aller fleste AI som et utfyllende verktøy i eksisterende systemer, mens bare 20 prosent ser det som en fundamental del av sikkerhetsarbeidet.

Denne tilbakeholdne tilnærmingen kan skyldes skepsis til AI-baserte sikkerhetsløsninger. Det er en bekymring knyttet til risikoen for falske alarmer, noe som kan føre til ineffektiv bruk av sikkerhetspersonellens tid. I tillegg anses mangelen på transparens i enkelte AI-systemer som problematisk, ettersom det kan skape usikkerhet rundt hvordan systemet tar beslutninger og gir anbefalinger. Videre kan generelle mangler i grunnforutsetningene for å jobbe med AI, som manglende kontroll og datahåndtering, føre til at virksomheter føler usikkerhet ved å introdusere AI-baserte sikkerhetsverktøy i miljøet.

AI OG MASKINLÆRING I CYBERSIKKERHETSARBEIDET⁹



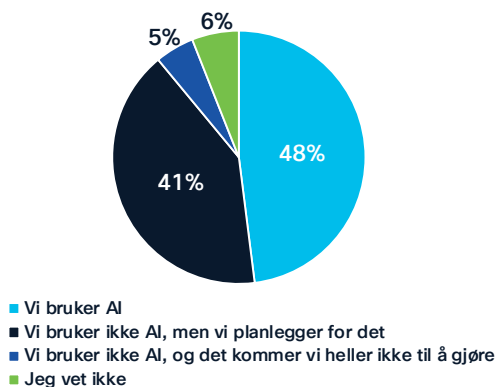
AI-reisen frem til nå

Det er tydelig fra både de ytre og indre faktorene at AI står høyt på agendaen, fra det høyeste politiske nivået helt ned til virksomhetene. Disse faktorene har på ulike måter preget arbeidet med AI frem til i dag og påvirker utviklingen fremover. Geopolitiske og regulatoriske svingninger, der de nye eksterne kravene og forutsetningene ennå ikke er helt definert, skaper usikkerhet rundt hvordan AI kan brukes i organisasjonen. Samtidig innebærer flere av utfordringene og kravene vi står overfor at AI vil måtte være en del av strategier fremover. Det er en kontinuerlig balansegang mellom fart og kontroll. I Sverige har det skjedd en tydelig markedspenetrasjon, men mye av den potensielle nytten gjenstår å realisere.

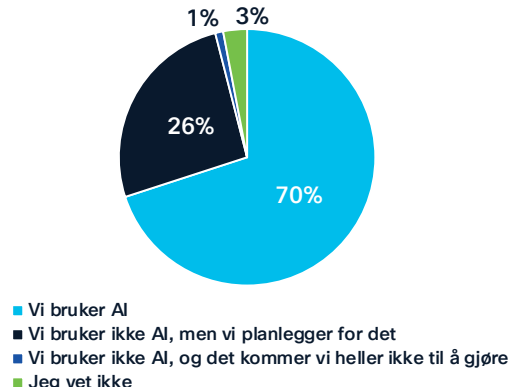
Bruksgrad og modenhet

AI har gjort et tydelig inntog i svenske virksomheter, og utviklingen skjer i stadig raskere takt. I 2024 oppga 48 prosent av svenske virksomheter at de brukte AI, og ytterligere 41 prosent oppga at de planla AI-implementeringer. Mye tyder på at disse planene nå er gjennomført, da hele 70 prosent av svenske virksomheter oppgir at de bruker AI i 2025, mens 26 prosent planlegger å bruke AI, noe som gjør den samlede andelen til 96 prosent. Også EUs evaluering av AI-KPI-er for 2025 peker på denne akselerasjonen, der Sverige viser en prosentvis økning av AI-brukende bedrifter på 142 prosent⁵, noe som kan sammenlignes med Danmarks 82 prosent³ og Finlands 61 prosent⁴.

AI-ANVENDELSE 2024⁸



AI-ANVENDELSE 2025⁸



Samtidig som svenske virksomheter utviser en høy bruksgrad av AI, er AI-modenheten generelt lav. Radars modenhetsmåling av svenske virksomheter, basert på faktorer som lederinvolvering, kompetanseutvikling og strategi, viser at sju av ti svenske virksomheter har en lav AI-modenhet. Blant disse befinner 23 prosent seg på det laveste nivået (nivå 1), mens 48 prosent befinner seg på det nest laveste nivået (nivå 2). Den høye bruksgraden sammen med den lave modenheten tyder på at mange organisasjoner fortsatt befinner seg i de tidlige fasene av sin AI-reise. Samtidig indikerer det faktum at drøyt dobbelt så mange organisasjoner befinner seg på nivå 2 sammenlignet med nivå 1, at vi delvis har forlatt den innledende «øve og prøve»-fasen, og at AI nå i større grad begynner å integreres mer systematisk i virksomhetene⁸.

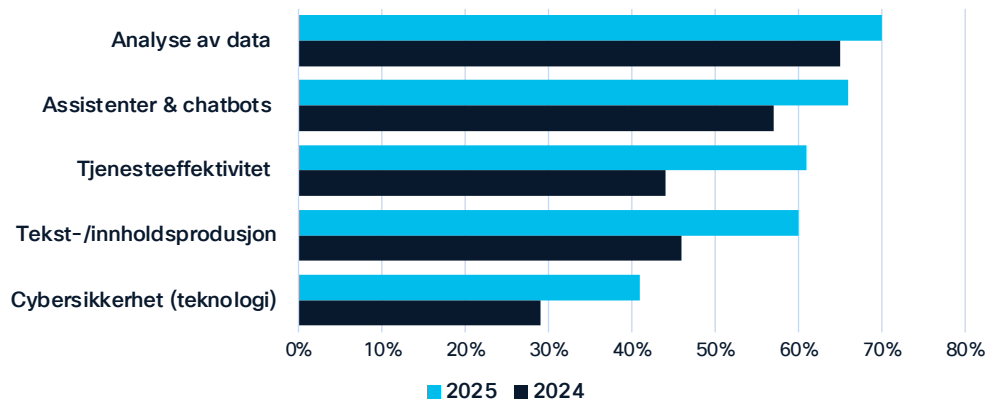
Nivå 4 Transformativ AI-modenhet (8%)	AI er integrert i organisasjonens strategi og driver operative og strategiske beslutninger. Skalerbar infrastruktur og robust datahåndtering er på plass, og AI er prioritert av ledelsen for å drive innovasjon og konkurransekraft. Avanserte analyser for forbedring samt kontinuerlig revisjon og risikostyring utføres.
Nivå 3 Operativ AI-modenhet (21%)	En velutviklet AI-struktur der teknologien brukes innen flere forretningsområder og bidrar til effektivisering og beslutningstaking. Infrastruktur, styring og overvåking er på plass, men kan optimaliseres, og det finnes et visst engasjement fra ledelsen.
Nivå 2 Grunnleggende AI-modenhet (48%)	Påbegynte prosjekter og initiativer med støttende infrastruktur og datastyring, men integrasjonen er begrenset, og det finnes utfordringer knyttet til skalerbarhet og kvalitet. Initiativer drives på avdelingsnivå og mangler kobling til forretningsstrategi.
Nivå 1 Umoden AI-organisasjon (23%)	AI brukes sporadisk, men uten en tydelig strategi. Det mangler AI-tilpasset data, styring, rammeverk og investeringer, samt engasjement og bevissthet fra ledelsen.

Dagens AI-verdiskapning

Det råder fortsatt usikkerhet rundt i hvilken grad AI faktisk skaper forretningsverdi og hva disse verdiene består av. Vurderingene spriker; en ekstern studie viste at konsulenter som brukte AI var mer produktive enn de som ikke gjorde det. De fullførte i gjennomsnitt 12 prosent flere oppgaver, jobbet 25 prosent raskere og leverte over 40 prosent høyere kvalitet enn kontrollgruppen¹. Samtidig peker en annen oppmerksom studie fra MIT på at 95 prosent av pilotprosjektene med generativ AI mislykkes⁷.

Hvilken verdi AI skaper, avhenger delvis av hvordan teknologien faktisk brukes. Virksomheter har beveget seg fra en hovedsakelig utforskende bruk av AI mot en mer anvendt fase. Fokus ligger i dag på effektivisering og automatisering, fremfor alt med generativ AI for ulike praktiske formål. 70 prosent av svenske IT-beslutningstakere oppgir at organisasjonen bruker AI til analyse av data, noe som er en marginell økning fra året før (65 prosent). Andre primære bruksområder for AI er assistenter og chatboter (66 prosent), tjenesteeffektivitet (61 prosent) og tekst- og innholdsproduksjon (60 prosent). Det er imidlertid tydelig at den generelle AI-bruken øker, da samtlige områder har en positiv utvikling siden i fjor.

DE 5 PRIMÆRE OMRÅDENE FOR NÅVÆRENDE OG PLANLAGT BRUK AV AI⁸



Verdiskapingen med AI vurderes i dag primært ut fra kvalitative snarere enn kvantitative grunnlag, noe som skyldes vanskeligheten med å måle AI sin faktiske avkastning. 44 prosent oppgir at det ikke foregår noen effektmåling eller evaluering av AI-prosjekter, mens ytterligere 43 prosent oppgir at virksomheten gjennomfører ad-hoc-evalueringer av AI-prosjekter uten etablerte måleparametere. Bare 2 prosent oppgir at de utfører en kontinuerlig evaluering med avansert analyse og overvåking. Dette er imidlertid et område der de nyttestyrte virksomhetene skiller seg fra de forventningsstyrte, der:

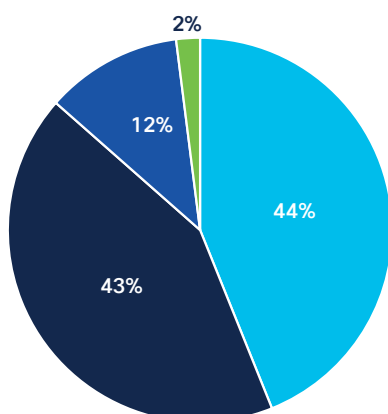
“Jeg ser på AI som et verktøy som får ting til å fungere mer effektivt, men det endrer jo egentlig ikke ansvaret.”

– CSO, privat sektor

Nyttestyrte virksomheter er **3x** mer tilbøyelige til å følge opp og måle effektene av sine AI-investeringer² (faktor)

Å ikke måle effektene av AI-investeringer risikerer å hemme utnyttelsen av gjennomførte investeringer, samt å forsinke nye satsinger, ettersom det skaper en følelse av at ressursene forsvinner uten tydelige resultater. Samtidig som svenske virksomheter forstår verdien av å hente ut gevinst fra sine AI-investeringer, identifiseres det tydelige hindre for dette.

OVERVÅKNING OG EVALUERING AV AVKASTNING PÅ AI-INVESTERINGER⁸



- Ingen formell effektmåling eller evaluering på plass.
- Ad-hoc-evaluering av AI-prosjekter uten etablerte måleparametere.
- Periodisk gjennomgang ved hjelp av definerte KPI:er for AI-ytelse.
- Kontinuerlig overvåking med avansert analyse og tilbakemeldingssløyfer.

Utfordringer med å overvåke og evaluere avkastningen på AI-investeringer

Det mangler ofte et tydelig bilde av normalsituasjonen ettersom målinger sjelden igangsettes i den utforskende fasen av AI-satsinger. Å vite når og hvor langt tilbake virksomheten bør måle i retrospektiv blir derfor utfordrende.

Det er vanskelig å isolere verdien av AI-initiativer fra andre initiativer, for eksempel omorganisering eller endring av roller.

Mye av verdien med AI i dag handler om effektivisering, noe som kan bygge på kvalitative og i visse tilfeller subjektive antakelser. Spesielt når det gjelder AI-baserte produktivitetstøytøy som brukes av individer.

Siden effektivitetsgevinsten for de vanligste anvendelsene ofte skjer på individnivå, er det vanskelig å fange opp organisatoriske nøkkeltall i form av målbar avkastning.

AI-reisen frem til i dag kan i stor grad anses å være preget av et forventningsstyrt perspektiv. Virksomheter utviser en høy bruksgrad, men bruksområdene handler i stor grad om individuell produktivitet og støtte til effektivisering, snarere enn å være fullt integrert i kjerneprosesser eller drive reell transformasjon. Til tross for at mange bruker teknologien, råder det en utbredt mangel på modenhet og en uklar kobling mellom AI-arbeid og verdiskaping. I takt med økende erfaring med den nye teknologien øker også kravene til å skape tydeligere verdier for virksomheten, og et nytt målbilde og en ny retning begynner å ta form.

AI-reisen fram til nå:

offentlig og privat sektor i sammenligning

AI-reisen, som hittil har kretset rundt generativ AI, har hatt visse forskjeller mellom privat og offentlig sektor. Forskjellene har i hovedsak handlet om grunnforutsetningene, som i sin tur har påvirket både muligheter og handlingsrom, og disse vil trolig øke når vi beveger oss mot morgendagens AI.

Forutsetninger

To grunnleggende forutsetninger som skiller privat og offentlig sektor, er ansvarsforhold og budsjettmessige rammer. Offentlig sektor preges av kravet om god etikk, tillit samt etterlevelse av demokratiske og juridiske prinsipper. Samtidig opererer sektoren innenfor en kompleks struktur med flere ytre krav og aktører å svare overfor. Man svarer oppover til politikken og lovgivningen, der politiske beslutninger bestemmer hvilke AI-initiativer som gjennomføres og innenfor hvilken tidshorisont. I tillegg svarer man utad til media og allmennheten, som begge overvåker og stiller krav til effektivitet, transparens og legitimitet.

Private virksomheter har en tendens til å prioritere prosessoptimalisering og har et sterkt forretningsdrevet fokus på inntektsstrømmer, kostnadsreduksjoner og på å teste ulike AI-anvendelser. Det er generelt en større fleksibilitet når det gjelder budsjett, utforming og prioriteringer av AI-initiativer, noe som henger sammen med at virksomhetene primært svarer overfor sine eiere, styre og kunder. Til forskjell fra offentlig sektor, der tildelingsbudsjetter er praksis og finansiering skiller seg mellom investering/innovasjon og forvaltning, er det innen privat sektor en høyere forventning om transformativ verdiskaping og avkastning på investering (ROI). Samlet sett skaper dette et forretningsmessig handlingsrom der AI-satsinger kan styres av lønnsomhet, konkurransekraft og markedsbegrep.

Muligheter og handlingsrom

Dette avdekker tre sentrale forskjeller mellom offentlig og privat sektor når det gjelder hvordan AI kan og bør brukes:

- 1. Muligheter til å ta del i nye løsninger.** En tydelig forskjell mellom privat og offentlig sektor er muligheten til å ta del i nye og innovative AI-løsninger. Siden private aktører generelt har færre lovkrav å forholde seg til og større budsjettfleksibilitet, er veien ofte kortere mellom idé og implementering. Flere offentlige aktører mener imidlertid at oppstartsselskaper (startups) og entreprenører, til tross for at de utvikler innovative og effektive løsninger, ikke alltid forstår de særskilte kravene som gjelder innen offentlig sektor. Lover som den svenske Offentlighets- og sekretesslagen (OSL) – tilsvarende bestemmelser i norsk offentlighetslov og forvaltningslov – har en tendens til å bli oversett, og det samme gjelder hvilke kriterier en virksomhet kan få unntak på. Selv om tjenesten kan være den samme som i privat sektor, må den derfor ofte tilpasses både i utforming og forretningsmodell ut

fra regelverkene som gjelder for den respektive sektoren.

2. AI-implementeringens dybde. Private virksomheter har generelt større fleksibilitet og handlingsrom når det gjelder bruksområder og dybden på AI-implementeringen. Hvilke AI-løsninger som brukes for de respektive forretningsområdene og funksjonene, samt hvor nær kjernevirksomheten de brukes, styres blant annet av tillit til teknologien, kompetanse, tekniske evner og forretningsnytte. Offentlige virksomheter må ta hensyn til de samme faktorene. Samtidig skjer bruken av AI ofte i sammenhenger som innebærer myndighetsutøvelse, rettighetsforvaltning og behandling av sensitive personopplysninger. Regelverk som likestillings- og diskrimineringsloven, forvaltningsloven, EUs AI-forordning og GDPR gjelder både offentlig og privat sektor, men får i praksis særlig betydning når AI tas i bruk i kjerneoppgaver og beslutningsprosesser i offentlig sektor. Gitt nåværende regelverk og hvordan AI-teknologien fungerer i dag, oppleves det som vanskelig innen offentlig sektor å bruke generativ AI i kjernevirksomheten og til saksbehandling. Dette er relatert til håndtering av personopplysninger og kravet om at beslutninger skal kunne granskes og spores. De samme begrensningene gjelder for agentisk AI, og det sentrale spørsmålet handler derfor ofte mindre om hvilken teknologi som brukes, og mer om i hvilken sammenheng den brukes.

3. Tillit fra kunde kontra tillit fra innbygger. Eftersom Siden offentlig og privat sektor svarer overfor ulike aktører, skiller bruksområdene og hvilke eventuelle risikoer man er villig til å ta seg fra hverandre. Private virksomheter håndterer sensitive data og beskytter dem ikke bare av sikkerhetshensyn, men også for å opprettholde tilliten fra kundene sine. Offentlige virksomheter svarer derimot overfor innbyggerne og mener at en eventuell datalekkasje kan få tillitsmessige konsekvenser som er betydelig vanskeligere å reparere. Offentlige aktører mener at private virksomheter, dersom tilliten skades, i verste fall kan avvikles, men også gjenoppstå i ny form. For offentlig sektor ser situasjonen annerledes ut, ettersom tilliten er vanskeligere å gjenvinne og handlingsrommet for en omstart er mer begrenset. I ny form. For offentlig sektor ser situationen annorlunda ut, ettersom förtroendet är svårare att återvinna och handlingsutrymmet för en omstart är mer begränsat.



“Hvis vi skader eller i ytterste konsekvens mister innbyggernes tillit i en dårlig AI-reise, skades tilliten til offentlig virksomhet alvorlig. Tillit er alfa og omega og høyest prioritert i alle situasjoner. Det er forskjellen sammenlignet med privat sektor”

– Digitaliseringsdirektør, svensk kommune

“Det er et felt i stadig endring, og vi må være raske med retningslinjer. Samtidig ønsker vi ikke å hindre eller begrense for mye. Men drivkraften vår er ikke nødvendigvis å ligge helt i front, men å velge de riktige prosjektene der vi kan høste fruktene av AI”

– CIO, privat sektor

Privat og offentlig sektors unike styrker

Privat sektor har en tendens til å bli oppfattet som mer drivende i AI-utviklingen, og private virksomheters fleksibilitet, fart og handlingskraft fremheves som nødvendig og til og med avgjørende for å sikre internasjonal teknologisk konkurransekraft. Kontrasten mot offentlig sektor er tydelig, da den ofte oppfattes som altfor regelstyrt, noe enkelte mener hemmer innovasjon, fart og transformasjon. Samtidig fremheves potensialet som ligger i offentlig sektors evne til å samordne innsats og samarbeide på tvers, en styrke som den private sektoren i mindre grad kan matche. To initiativer som løftes frem som spesielt viktige for å drive Sveriges offentlige AI-reise fremover, er deres *Samordnad statlig IT-drift* og *AI-verkstaden*.

SAMORDNET STATLIG IT-DRIFT

I Sverige utgjør Försäkringskassan, Trafikverket, Skatteverket og Lantmäteriet den såkalte firkløveren, som har i oppdrag å samordne et statlig tjenestetilbud for IT-drift. Formålet er å skape en effektiv, sikker og ensartet håndtering av statens IT-driftstjenester, noe som gir betydelig potensial for blant annet datalagring, infrastruktur og cybersikkerhet. Disse myndighetene, med høy cyberkompetanse og omfattende erfaring med IT-drift, kan tilby slike tjenester til andre myndigheter, noe som i sin tur øker både kostnadseffektiviteten og sikkerheten.

Oppdraget om en samordnet statlig IT-drift beskrives dessuten som en forutsetning for AI-verkstedet, der to svenske myndigheter – Skatteverket og Försäkringskassan – begge deltar i initiativet.

AI-VERKSTEDET

Försäkringskassan og Skatteverket har fått i oppdrag av regjeringen å utrede forutsetningene for et AI-verksted for offentlig sektor. Formålet er at offentlige aktører skal kunne utvikle, dele og forvalte AI-løsninger med hverandre. Løsningen sparer tid og penger, styrker cybersikkerheten og gir mindre aktører mulighet til å benytte AI-kapasitet uten å måtte bygge opp egen AI-kompetanse. En IT-direktør ved en myndighet beskriver det som:

“et koldtbord av muligheter for oss myndigheter”

AI-verkstaden har potential att bli ett viktigt steg mot ökad digital suveränitet utan att kompromissa med snabb skalbarhet. AI-verkstaden fungerar som en garant för en säker symbios mellan respektive myndighet, region eller kommun och den statliga AI-verkstaden. Den kommer drivas inom en säker och kontrollerad infrastruktur, med erforderlig kompetens och vara i linje med de regulatoriska krav och behov som offentlig sektor måste följa, samtidigt som respektive aktör kan bibehålla egen autonomi och rådighet över utvalda delar.



Målbildet for en AI-drevet fremtid

AI har i dag både høy prioritet og høy bruksgrad, men for å gire opp verdiskapingen må den fremtidige AI-reisen bygges på en annen måte enn den har blitt gjort hittil. Den fremtidige verdiskapingen med AI bygger på ulike sentrale prinsipper og tilnærmingsmåter:

Fra teknnologidrevet til strategisk forankret

Det utforskende arbeidet med AI har skapt innsikt og begynt å etablere interne evner og struktur hos virksomheter. Det råder imidlertid fortsatt et utpreget teknologiperspektiv der arbeidet med AI ofte er frakoblet, eller bare svakt koblet til virksomhetsstrategier. For å lykkes bedre med å skape virksomhetsnytte med AI og bidra til reell endring, må virksomheter begynne innenfra og evaluere hvordan AI kan bidra til å nå virksomhetens mål. For å lykkes med skiftet fra forventningsstyrt til nyttestyrt, må arbeidet ta utgangspunkt i:

- 1. Strategi** – som definerer den fremtidige forretningen eller virksomheten og hvordan den skal oppfattes av markedet, kunder, brukere eller innbyggere.
- 2. Tjenstedesign** – som spesifiserer hvilke tjenester som trengs for å kunne levere i henhold til strategien.
- 3. Tekniske evner** – som kreves for å levere de nødvendige tjenestene.
- 4. Operativ modell** – som beskriver prosessene, arbeidsmåtene, styringen og ressursene som kreves for å skape verdi og nå de strategiske målene i organisasjonen.

De tjenestene som kreves for å realisere fremtidige strategier, forutsetter nye tekniske evner. Når AI derimot blir et selvformål og ikke kobles til virksomhetens mål, forsvinner mye av den potensielle verdien. Fokus må derfor ligge på hvilke problemer og målsettinger som skal løses, og hvordan teknologi, prosesser og styring sammen kan muliggjøre dem. Uten denne koblingen risikerer AI-satsinger å bli kostbar signalpolitikk snarere enn reell utvikling.

Flyttes til neste side

Det er en økende innsikt om at arbeidet med generativ AI ikke har skapt tydelige virksomhetsverdier, men snarere har oppnådd effekter på individnivå for medarbeidere som kan løse hverdagsproblemer med høyere effektivitet. En utfordring ligger i at de store sentrale språkmodellene (såkalte foundational models) er altfor generiske og dermed mangelfulle når det gjelder å løse spesifikke virksomhetsproblemer. Når virksomheter skifter fra et teknisk til et strategisk perspektiv, øker behovet for løsninger som er mer spesifikke, mer virksomhetsnære og mer varierte. Generiske modeller kan ikke matche virksomhetsunike problemer på best mulig måte, noe som medfører et økt behov for tilpasninger eller videreutvikling, og dette kan skje på ulike måter:

Metode for tilpasning	Beskrivelse	Innsats for virksomheter
Prompt engineering	Påvirke og styre modellens utdata ved å arbeide med spesifikke instruksjoner (prompts)	Relativt ressurseffektivt og mulig å gjøre i egen virksomhet
RAG (Retrieval augmented generation)	Komplettering av en modells treningsdata med godkjente og relevante eksterne kunnskapskilder for å skape mer nøyaktige og pålitelige svar	Resultatet avhenger av tilgangen på eksterne data med god kvalitet som brukes til å gi modellen kontekst, men det er en relativt effektiv måte å forbedre generative AI-modeller på
Finjustere eksisterende modeller	Trening av eksisterende modeller på egne data for mer spesialiserte anvendelser	Ikke like krevende som å trene en modell fra grunnen av, men krever fortsatt både data og beregningskraft
Trene egne modeller	Utvikle og trene en stor språkmodell (LLM) fra grunnen av	Krever enorme mengder data, noe som gjør dette alternativet uoppnåelig for de fleste virksomheter

Hvilke metoder som vil bli benyttet, vil variere for ulike virksomheter avhengig av behov og forutsetninger. Denne typen tilpasning tar imidlertid utgangspunkt i de språkmodellene som finnes i dag, men de fremtidige kravene til en mer transformativ verdiskaping vil også bli bygget på andre tekniske evner.

Fra individ til virksomhet

Med skiftet fra de sentrale generiske modellene til et målbilde som inneholder mer virksomhetsspesifikke løsninger, skapes det også en forventning om verdiskaping som skifter fra individ til virksomhet. Med et mer strategisk, virksomhetsnært og prosessorientert perspektiv skapes muligheter for både større og andre typer verdier. Høyere krav til verdiskapingen stiller imidlertid også høyere krav til de tekniske evnene som skal muliggjøre dette. Mer spesifikke modeller trent på virksomhetens data kan være et første steg, men den eksponentielle verdiskapingen vil kunne muliggjøres av agentisk AI. Det vil si når systemene blir mer autonome og selvstendig kan agere mot mål og bryte ned, planlegge, beslutte og utføre oppgaver.

Generativ AI	Agentisk AI	Agentnettverk ("mesh")
Stor språkmodell som utnytter data for å skape nytt innhold som tekst, bilde, lyd eller kode	Autonome systemer som agerer selvstendig for å løse komplekse problemer i flere trinn	Sammenkoblet økosystem der autonome AI-agenter samarbeider i desentraliserte systemer
Output-orientert og reaktiv. Skaper innhold basert på instruksjoner (prompt)		Målorientert og proaktiv. Løser selvstendig komplekse problemer
Økt produktivitet og effektivitet, spesielt for individer		Skalerbar transformativ verdiskaping, frigjøring av menneskelig kapasitet
Sentrale store modeller som krever mengder data, beregningskraft og energi		Desentralisering, mindre og mer spesialiserte modeller

“Hvis vi skal bygge reelle verdier, må vi slutte å være så teknologidrevne. Når man sier at man skal bygge agentnettverk, er man fortsatt låst i teknologien. Det må drives av forretningen og behovene – hvor skal vi være om 10 år – og lage en plan for det. Sannsynligvis er AI-agenter med i løsningen, men vi skal ikke begynne i den enden.”

– VD, privat sektor

Nettverk av AI-agenter vil ikke kunne løse alle problemer, men det muliggjør fremtidige evner som dagens generative AI ikke har en sjanse til å kunne realisere. Snarere enn det sentraliserte og generiske, bygger agentisk AI på en distribuert arkitektur med høyere grad av fleksibilitet som gjør løsningene mer virksomhetsnære. Det skaper muligheter for å kunne utnytte teknologien til mange ulike bruksområder og å kunne skalere produksjonen basert på behov. Til tross for at teknologien innebærer mange nye muligheter, må den strategiske forankringen fortsatt definere hvordan den kan og bør brukes av virksomheter.

Fra innelåsing til kontroll

Forståelse og kontroll over virksomhetens data er grunnforutsetninger for å lykkes med de mer virksomhetsspesifikke AI-anvendelsene, både når det gjelder tilpasning av eksisterende modeller og arbeid med agentnettverk. Både den geopolitiske og regulatoriske utviklingen med fokus på suverenitetsspørsmål har drevet frem en økt innsikt i at mange virksomheter mangler både råderett over og tilstrekkelig innsikt i hvilke krav til konfidensialitet, riktighet, tilgjengelighet og sporbarhet egne data har. Manglende rutiner rundt informasjonsklassifisering vanskeliggjør også utformingen av et effektivt sikkerhetsarbeid og kan bidra til at mange virksomheter føler usikkerhet rundt å inkorporere AI i sikkerhetsstrategien..

Når AI integreres i kjerneprosesser og blir tydeligere koblet til virksomheten, oppstår det et økt behov for kontroll. Virksomheter uttrykker et behov for økt kontroll over data og infrastruktur, samt økt innsyn i modeller for å sikre råderett over det som er mest virksomhetskritisk. Det innebærer imidlertid ikke at virksomheter ønsker å ta hjem og kjøre all IT-produksjon i egen regi. Det som avgjør veien videre, er fremfor alt avveininger knyttet til egen evne samt tid. Virksomheter må ta stilling til egne evner og dermed hva som er ønskelig og realistisk å gjøre selv. Dette gjelder spesielt evner og forutsetninger rundt infrastruktur, kompetanse, budsjett samt cybersikkerhet. I tillegg må virksomheter forholde seg til tidsaspektet. Det er viktig å utvikle seg i rask takt for både å styrke konkurransekraft og motstandskraft mot eksterne faktorer, og for å beskytte virksomheten mot risiko.

Et økt fokus på kontroll og en økende modenhet rundt datahåndtering vil medføre et skifte mot mer hybride og varierte oppsett, der de mest sensitive eller kritiske eiendelene kan håndteres annerledes basert på behov. Innelåsingeffekter forsøkes unngått i størst mulig grad, og fleksible oppsett premieres i leverandørforholdet.

Gårdagens reise	Morgendagens reise
Teknologidrevet	Strategisk drevet
Generiske og generelle AI-modeller	Mer spesifikke og virksomhetsnære AI-modeller
Individuell produktivitet	Transformative virksomhetsverdier
Sentrale modeller i gigantiske datasentre som krever mengder av ressurser	Distribuerte modeller som kjøres nærmere brukerne på lokal infrastruktur
Data, sikkerhet og prosesser i vertikale siloer	Horisontale dataflyter koblet til kjerneprosesser og med integrert sikkerhet
Innelåsing og manglende handlingsrom	Oversikt, kontroll og fleksibilitet

En helt ny verdiskaping

Drivkraften for å skifte fokus fra det forventningsstyrte til det nyttestyrte, og å arbeide i tråd med prinsippene og tilnærmingsmåtene som har blitt diskutert i dette kapittelet, er at virksomheten ønsker å oppnå en mer omfattende og transformativ verdiskaping. Virksomheter ønsker å ta neste steg fra den utforskende fasen der idéer testes og valideres, til å bygge AI-drevne kapabiliteter integrert i kjerneprosessene med mulighet for å skalere opp produksjonen over tid. Felles for virksomhetene som ligger lengst fremme og har et tydeligere nyttestyrt perspektiv, er et syn på verdiskaping med AI i form av økt lønnsomhet og nye inntektsstrømmer, snarere enn som et verktøy for kostnadsreduksjon og sparing.

En studie gjennomført over flere år, som har undersøkt forskjellen mellom virksomhetene som har lyktes best sammenlignet med markedsgjennomsnittet, kan påvise tydelige verdigevinster innen flere ulike områder for de ledende virksomhetene². Felles for disse virksomhetene er en systematisk arbeidsmåte rundt AI som hviler på et strategisk grunnlag, med tydelig styring, samt god balanse mellom organisatoriske og tekniske områder. Disse verdiene kan ses på som eksempler på hva som kan oppnås gjennom en mer strategisk, verdidrevet og virksomhetsfokusert AI-reise.

Virksomhetsverdier som rapporteres av virksomhetene som ligger lengst fremme og har et nyttestyrt perspektiv, sammenlignet med markedsgjennomsnittet².

FORSTERKET KONKURANSEKRAFT

1,5x

Økte inntekter
Økt lønnsomhet

NYE MARKEDER

+30%

Nye inntektsstrømmer
Lanserte nye produkter & tjenester

FORBEDREDE OPPLEVELSER

+25%

Forbedret kundeopplevelser
Forbedret produktivitet i teamene

RASKERE TAKT

4x

Flere som har ferdigstilt sine brukstilfeller

Virksomheters ambisjoner om å nå disse verdiene stiller nye krav til de tekniske verktøyene, men det skaper også behov for nye underliggende kapabiliteter. Hvis det fremtidige målbildet for AI-reisen baseres på et mer strategisk og virksomhetsnært grunnlag, med høyere krav til kontroll og råderett og som skal generere tydeligere virksomhetsverdier, så får det implikasjoner i flere ulike dimensjoner. Reisen mot målet vil kreve innsats som berører både mennesker, virksomhet og teknologi.

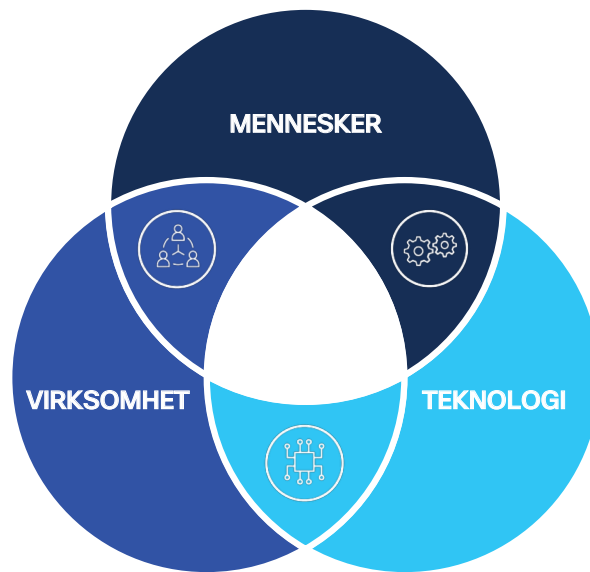
Endringsreisen mot målbildet

Målbildet styres av virksomhetsbehov

Den fremtidige AI-reisen bygger på en ny måte å se på verdiskaping, men vil påvirkes av virksomhetens formål, forutsetninger og ambisjonsnivå. Hver virksomhet må definere sitt eget spesifikke målbilde, blant annet ut fra behovet for kontroll, ytelse, innsyn og kompetanse, og hvordan morgendagens AI kan bidra til å muliggjøre dette. Det strategisk forankrede målbildet vil avgjøre den endringsreisen som hver organisasjon står overfor.

Utfordringer og muliggjørere

Brukstilfeller og teknologivalg kan variere, men koblingen mellom mennesker, prosess og teknologi skaper forutsetningene som kreves for å kunne skape verdi. I endringsreisen handler neste steg ikke bare om å forstå hva AI kan gjøre, men om å identifisere hva som kreves for å komme dit. Med dagens utgangspunkt som base og målbildet i sikte, må virksomheter forstå hvilke faktorer som muliggjør denne reisen, og hvilke som risikerer å holde den tilbake. Enkelte faktorer eller problemstillinger har virksomheter håndtert over lengre tid, men disse krever nå en helt ny tilnærming, mens andre er helt nye. Les videre med din egen virksomhet i tankene: identifiser deres sterkeste område og pek ut hvor de tydeligste behovene finnes.



MENNESKER

Det er menneskets forståelse, kompetanse og evne som avgjør hvordan AI utvikles og brukes fremover. Mye av fokuset i diskusjoner om AI legges på virksomheten eller tekniske aspekter, men for at virksomheten skal lykkes med sin AI-transformasjon, må også menneskelige faktorer tas i betraktning. Det gjelder alt fra konkrete til myke eller til og med eksistensielle spørsmål.

VIRKSOMHET

For å ta neste steg i AI-reisen kreves en virksomhet som gir retning og struktur. Tydelig lederskap, strategi, mot og samhandling er avgjørende for å gå fra enkeltinitiativer til en mer systematisk arbeidsmåte som skaper organisatorisk verdi. Når dette mangler, risikerer arbeidet med AI å bli fragmentert og ineffektivt.

TEKNOLOGI

Nye tekniske kapabiliteter vil kreves for å muliggjøre en forflytning inn i neste æra av AI, der tilgang til kvalitetsdata er en grunnforutsetning for å lykkes. AI-modeller som trenes på egne data eller utfører oppgaver nærmere brukerne, stiller store krav til både infrastruktur og sikkerhetsarkitektur, samtidig som det åpner for suverenitetsspørsmål.

Mennesker

TILLIT

Tillit er både en forutsetning og en utfordring i endringsreisen mot morgendagens AI, ettersom tilliten til teknologien i stor grad avgjør om den faktisk vil bli brukt i praksis. For å bygge tillit til modellenes beslutninger eller resultater kreves innsyn i hvordan modellene oppfører seg innenfor gitte rammer – hvor ofte de tar feil og hvordan de reagerer på motstridende eller ondsinnede instruksjoner. Når tilliten uteblir, risikerer teknologien å forbli på pilotstadiet eller bli brukt på en måte som skaper usikkerhet snarere enn verdi. Manglende tillit fører til forsiktighet og manuelle omveier,

noe som blir spesielt kontraproduktivt i et miljø med autonome systemer. På tilsvarende måte må tillit også balanseres med kritisk tenkning. Spesielt med dagens generative AI-modeller er det en tendens til å se på modellen som en bevissthet, og den menneskelige og tillitvekkende tonaliteten skaper en, til tider, overvurdert tillit til resultatet.

Brukere må forstå hvordan verktøyene fungerer, hvilke risikoer som finnes og hvilke kontroll-steg som beskytter dem. Bekymring rundt arbeidsoppgaver, ansvar og kvalitet må adresseres åpent. En vellykket vei fremover er ofte en pragmatisk kombinasjon av menneske og teknologi, der tilbakemeldinger fra brukere forbedrer modellene, og der roller som produkt-, data- og modelleiere har tydelige mandater. Tillit og tiltro bygges i det lange løp ikke bare gjennom policyer, men gjennom erfaring, opplæring og praktisk bruk.

83% vurderer at risikoen for **spredning av feilaktig informasjon** ved bruk av AI er **høy** eller **ganske høy**⁸.

KOMPETANSE

Resultatet av virksomhetens AI-arbeid påvirkes av hvordan teknologien brukes i praksis, noe som gjør menneskets kompetanse og kunnskap til en grunnleggende forutsetning for endringsreisen. I takt med at AI integreres tettere på virksomhetens kjerneprosesser, forskyves kravene fra teknisk kunnskap til evnen til å forstå og tolke hvordan de nye systemene fungerer, tar beslutninger og samhandler i miljøet..

Når AI blir mer avansert og tas i bruk mer virksomhetsnært, kreves det samtidig et kollektivt kompetanseløft i organisasjonen for både å skape forutsetninger for å få verdi ut av teknologien, men også for å sikre at den brukes korrekt ut fra et risiko- og sikkerhetsperspektiv. Dagens situasjon viser to relaterte problemer: modenheten og kompetansen er for lav på individnivå, og modenheten og kompetansen er ujevn på virksomhetsnivå. I dag oppgir 38 prosent av IT-beslutningstakerne at det ikke finnes noe spesifikt fokus på AI-kompetanse og ferdighetsutvikling, og ytterligere 36 prosent oppgir at det foregår sporadisk opplæring. Bare 13 prosent oppgir at det enten finnes dedikerte AI-team eller en helhetlig strategi for utvikling av AI-kompetanse. Slike handlingsplaner eller strategier skaper viktige forutsetninger for å ta neste steg i AI-reisen.

I tillegg til dette er modenheten og kompetansen ujevn på virksomhetsnivå. Mye av dagens AI-bruk er individstyrt og drives av enkelte ildsjeler. De som er interessert, søker selv kunnskap og utvikler seg raskt, mens øvrige medarbeidere kun får den begrensede kompetansehevingen som virksomheten tilbyr.

ORGANISASJONENS SYN PÅ AI-RELATERT TALENT OG KOMPETANSEUTVIKLING⁸



INTELLEKTUELL RÅDERETT

Råderett og suverenitet handler ikke bare om geopolittikk og regulatoriske rammeverk, men også om menneskets intellektuelle evne og kunnskap. I dag foregår diskusjonen om intellektuell råderett og suverenitet delvis innen utdanningssektoren, der det er en bekymring for at den yngre generasjonen, gjennom omfattende AI-bruk i skolen og på universitetet, vil miste deler av sin kritiske tenkning og problemløsningsevne.

I takt med at AI-systemer blir mer integrert i kjerneprosesser og blir mer selvgående, vil denne diskusjonen måtte tas innad i virksomhetene. Hvis mennesket blir altfor avhengig av teknologien, risikerer man en form for intellektuell innelåsning og tap av eierskap, der forståelsen for beslutningene flyttes fra menneske til maskin.

Ut fra det perspektivet blir kompetanseutvikling igjen høyaktuelt, ettersom det blir nødvendig å bevare menneskelig kontroll over AI og dens beslutningstaking. For å kunne akselerere AI-reisen på en sikker og bærekraftig måte, må virksomhetene derfor stille seg to sentrale spørsmål: Hvilken kunnskap og evne må vi ha selv, og hva kan vi overlate til en modell?

ANSVAR

Etter hvert som AI-systemene blir mer autonome og mer involvert i beslutningstaking, øker kravene til ansvar og ansvarsutkreving, noe virksomheter må ta hensyn til for å gjennomføre sin AI-reise på en sikker og kontrollert måte. Ansvarstaking og ansvarsutkreving blir mer komplekst når mennesker og teknologi samhandler og jobber tett sammen. Det finnes en menneskelig tendens til å unngå ansvar, og som tidligere nevnt, påpeker enkelte risikoen for at ansvaret for utfallet legges på teknologien og at AI brukes som en syndebukk.

I dag er ansvar for beslutninger, budsjett og styring spredt i organisasjonen, fra IT-avdelingen til toppledelsen og linjeorganisasjonen, noe som stiller krav til tydelige strategier, retningslinjer (policys) og samarbeidsfora for å få helheten til å henge sammen. Når nye AI-verktøy ruller ut til medarbeiderne, må det derfor finnes en tydelig plan og et klart definert mandat for hvordan teknologien kan brukes, slik at muligheter for kreativitet, innovasjon og problemløsning balanseres med beskyttelse mot sikkerhetsrisiko og feil. Regler for bruk, beskyttelsesmekanismer og en tydelig etablert beskrivelse av hva et AI-system har lov til å gjøre, og hvem som er øverst ansvarlig for disse beslutningene, er derfor nødvendig.



MENNESKELIGE MULIGGJØRERE

TILLIT

Tillit og tiltro til AI avgjør om og hvordan teknologien vil bli brukt. Samtidig kreves det bevissthet om hallusinasjoner eller ondsinnet bruk.

- Transparens rundt formål og mål med AI-bruken
- Informasjon om hvordan modellene fungerer og tar beslutninger
- Tillit gjennom praktiske erfaringer

KOMPETANSE

AI-kompetanse trengs på alle nivåer i organisasjonen for å kunne jobbe med verktøyene på en effektiv og sikker måte.

- Strategi for talentutvikling (tilgang på talenter)
- Opplæring og kompetanseutvikling
- Bruke metoder og verktøy for å drive endringsledelse

RÅDERETT

Bevar kontroll og råderett over kritiske kapabiliteter eller kompetanser for ikke å havne i en intellektuell innelåsning.

- Praktisere kritisk granskning og kildekritikk for AI
- Strategi for kapabilitetsutvikling som omfatter både mennesker og teknologi
- Redundans for de mest kritiske kapabilitetene

ANSVAR

I samspillet mellom menneske og teknologi, og spesielt for mer autonome AI-systemer, øker kravene til tydelighet rundt ansvar og mandat.

- Tydelige strategier, retningslinjer (policys) og samarbeidsfora
- Regler for bruk og beskyttelsesmekanismer
- Tydelig eierskap over AI-baserte beslutninger

Virksomhet

LEDERSKAP

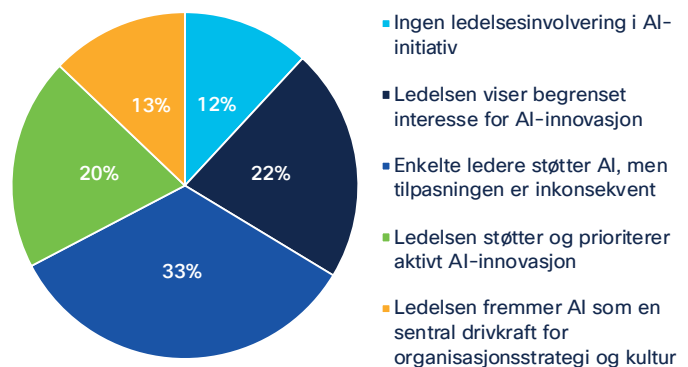
Sterkt lederskap er en avgjørende faktor for å ta AI fra punktvisse initiativer til en helhetsintegret del av virksomheten. Ved å gå foran som et godt eksempel og prioritere kompetanseutvikling og opplæring, kan ledelsen legge til rette for at AI brukes på en strukturert, sikker og langsiktig måte. Når lederskapet uteblir, skjer ofte det motsatte – arbeidet blir dårlig samordnet, endringen møter motstand fra medarbeidere og løsninger forblir midlertidige. I dag er ledelsens involvering i AI-initiativer begrenset, og 12 prosent av IT-beslutningstakerne oppgir at det ikke finnes noen involvering, mens ytterligere 22 prosent oppgir at ledere viser begrenset interesse for AI-innovasjon.

Fremover vil det ikke bare kreves en bredere involvering fra ledelsen, men også et lederskap som mestrer nye krav. Når systemene blir mer autonome og agerer selvstendig for å løse komplekse problemer, vil dynamikken på arbeidsplassen endres, noe som stiller høyere krav til lederens tekniske, sosiale og emosjonelle ferdigheter. Interaksjonen vil gå fra menneske-menneske til både agent-menneske og agent-agent. Fra bare å lede og oppmuntre mennesker til en sikker AI-bruk, til også å lede agenter som samarbeider med hverandre og med mennesket. Dette krever et lederskap som forstår teknologiens logikk, men som også har evne til empati og forståelse for menneskets behov og følelser.

“Det er et kulturskifte at medarbeidere skal forstå det samme – at vi må drive en rask og intensiv utvikling på tvers av våre systemer og arkitektur”

– IT-direktør, svensk myndighet

LEDELSESINVOLVERING I AI-INITIATIVER⁸



STRATEGI

En nyttestyrkt virksomhet orkestrerer et effektivt samspill mellom de tekniske kapabilitetene, prosessene og operative modellene som underbygger dem, samt den menneskelige kompetansen og evnen som kreves for bruken. For å få helheten til å henge sammen, kreves en strategi som kobler sammen alle disse områdene, og som henger sammen med den overordnede virksomhetsstrategien.

At AI må være forankret i det strategiske arbeidet, er det ingen tvil om. Derimot er det delte meninger om hvorvidt det bør finnes en egen AI-strategi eller ikke. En separat strategi for et spesifikt teknikkområde risikerer å føre til en teknikkorientert tilnærming, men samtidig kan AI-teknologiens spesielle og transformative rolle skape behov for en dedikert strategi for å skape retning, ansvar og samordning.

I takt med at AI blir mer virksomhetsnært og påvirker hvordan organisasjonen styres og organiseres, kreves en fremtidsrettet strategi som omfatter hvordan AI kan integreres i virksomhetsprosesser og bidra til å utvikle virksomheten og dens tjenester. Per i dag er det imidlertid svært få som har utviklet en slik helhetsstrategi. Bare 4 % oppgir at det finnes en integrert AI-styring gjennom hele organisasjonen⁸.

4% oppgir at det finnes en **integrert AI-styring** gjennom hele organisasjonen⁸.

Det finnes imidlertid tegn på at AI-arbeidet i mange tilfeller er frikoblet fra altfor rigide eller strenge strukturer. Det preges ofte av fleksibilitet og mindre formelle strukturer der virksomheter delvis har sluppet noe på ambisjonen om å få total kontroll over medarbeidernes AI-bruk. Initiativer kommer både ovenfra og nedenfra, og mye handler om å tillate egne initiativer og ildsjeler for å fremme snarere enn å hemme innovasjonskraft.

Siden dagens AI-strategi formes både ovenfra og nedenfra, blir ledelsens engasjement avgjørende, spesielt når kravene og initiativene kommer nedenfra. Her oppstår en synergieffekt; virksomheter med høy ledelsesinvolvering og en velutviklet strategi har bedre forutsetninger for å drive sin forflytning mot en mer integrert og organisatorisk verdiskapende AI-bruk. For organisasjoner som mangler begge disse komponentene, risikerer utviklingen derimot å stoppe opp.

Like viktig som at AI-reisen er drevet av organisasjonens overordnede strategi, er det å ha en tilpasset og optimalisert operativ modell. Mest sannsynlig er den eksisterende operative modellen ikke optimalisert for neste fase av AI-reisen. Når virksomheter blir stadig mer nyttestyrte, stilles det nye krav til den operative modellen for å oppnå tydelighet rundt prioriteringer, øke farten og bidra til kraft og engasjement for flere AI-initiativer. Nye tekniske kapabiliteter vil også medføre at forvaltningsmodellen i den operative modellen må gjennomgås. Behovet er utbredt og treffer virksomheter uavhengig av sektor eller hvor moderne dagens IT-infrastruktur er.

2/3 av organisasjonene oppgir at de har oppdatert sin operative modell for å få mer tilpassede AI-kapabiliteter⁶.

Det som kjennetegner den operative modellen hos de virksomhetene som har lyktes best, er en høy beredskap og fleksibilitet for nye risikoer eller hendelser som påvirker organisasjonen. Det gjør det lettere å raskt omstille seg og snu endrede forutsetninger til muligheter. De ledende virksomhetene prioriterer dessuten innovasjonsevne, strategisk håndtering av sine data samt teknisk kapabilitet i den operative modellen. En velfungerende operativ modell for neste fase i AI-reisen kjennetegnes av:

TYDELIGHET

Ansatte, ressurser og ansvar er i tråd med virksomhetsstrategien

FART

Beslutningsprosesser, arbeidsflyter og prosesser er teknologiforsterkede og effektive

EVNE

En fremtidssikret organisasjon har evne til å levere andre verdier enn tidligere

ENGASJEMENT

En resultatorientert kultur som bygger på tydelighet, fart og evne bidrar til høy motivasjon

MOT

Mot handler dels om å gi medarbeiderne rom til å bruke og utforske AI-løsninger, og dels om å tørre å drive forflytningen fremover. Det første steget i mange virksomheters AI-reise har handlet om å la medarbeiderne «øve og prøve» – noe de aller fleste allerede har gjort, gitt den høye bruksgraden.

Å drive AI-reisen fra dagens generative AI til morgendagens autonome systemer krever imidlertid en helt annen form for mot. Å strebe mot de større verdiene som AI kan skape, innebærer å satse på sin AI-reise med fokus på transformasjon snarere enn bare effektivisering, noe som krever mot til å utfordre vante arbeidsmåter. Svenske beslutningstakere kan identifisere hvor de største verdiene finnes og hvordan de kan oppnås, men er bekymret for hvilke konsekvenser det kan få for virksomheten og dens medarbeidere. Også regulatoriske krav bidrar til en usikkerhet rundt det å akselerere AI-reisen, ettersom det er uklart hvor langt virksomheten faktisk kan gå og hva som er tillatt.

“Det er en usikkerhet og bekymring rundt hvor langt vi kan gå eller tør å gå, for ingen vil jo gjøre feil”

– IT-direktør, svensk offentlig myndighet

SAMHANDLING

Samarbeidsklimaet er helt avgjørende for hvor godt vi vil lykkes med å skape verdier med AI som virksomheter og samfunn. Det er mye som er utforsket og nytt, og for å overvinne hindre kreves det at vi tar de riktige diskusjonene. Koblet til betydningen av mot, må vi bygge arenaer der vi tør å blotte vår manglende kunnskap. Først da kan en reell forflytning oppnås. Det er ofte enklere og mer vanlig å dele det som har gått bra, men det å tørre å snakke om det usikre og løfte spørsmål uten enkle eller tydelige svar, kan utgjøre et enda bedre grunnlag for konstruktive dialoger. Svenske (og norske) virksomheter og organisasjoner har en tradisjon for samhandling som skiller seg fra mange andre land, og det er en styrke som bør utnyttes og forsterkes nå. Et godt utgangspunkt er å identifisere virksomheter eller områder som ikke står i direkte konkurranse, og bygge diskusjon og samarbeid ut fra det.

Samhandling mellom organisasjoner vil ikke bare være en viktig nøkkel, men også samhandling innad i organisasjoner. Først når ulike individer, roller og funksjoner har et felles syn på fremtiden og jobber i samme retning, vil de virkelige verdiene kunne skapes.



VIKSOMHETSMESSIGE MULIGGJØRERE

LEDERSKAP

Mer autonome AI-systemer vil stille høyere krav til lederes tekniske, sosiale og emosjonelle evner.

- Øk ledelsens engasjement og ansvar i AI-arbeidet
- Invester i kompetanseutvikling for ledere
- Utvikle et nytt lederskap for agentbaserte arbeidsmiljøer

STRATEGI

En fremtidsrettet strategi omfatter hvordan AI kan integreres i virksomhetsprosesser og bidra til å utvikle virksomheten og dens tjenester.

- Utvikle en helhetsstrategi som integrerer AI i virksomhetens mål, prosesser og styring
- Skap en fleksibel strategisk modell som kombinerer sentral retning med desentralisert innovasjon
- Oppdater og tilpass den operative modellen

MOT

Å strebe mot de større verdiene som AI kan skape, krever fokus på transformasjon snarere enn bare effektivisering, noe som krever mot til å utfordre vante arbeidsmåter.

- Skap strukturer som gjør det trygt å eksperimentere
- Prioriter initiativer som driver transformasjon, ikke bare effektivisering
- Utvikle tydelige veiledninger for å redusere regulatorisk usikkerhet

SAMHANDLING

Det er mye som er utforsket og nytt, og for å overvinne hindringer kreves det at vi tar de riktige diskusjonene sammen.

- Bygg arenaer der man tør å blotte sin manglende kunnskap
- Identifiser virksomheter og områder som ikke er i konkurranse, og bygg samhandling ut fra det
- Styrk samhandlingen innad i organisasjonen

Teknologi

DATA

Data er en forutsetning for arbeidet med AI og kan være både en flaskehals og en muliggjører for å lykkes med de virksomhetsnære anvendelsene. Utfallet avhenger av virksomhetens arbeid med informasjonsklassifisering, men også av tilgangen til og kvaliteten på data.

Informasjonsklassifisering har lenge vært utfordrende for virksomheter, noe som har blitt forsterket i takt med en økende digitaliseringsgrad, med en økende datagenereringstakt som følge. Når virksomheten begynner å arbeide med å implementere AI, blir manglene i datahåndteringen synliggjort og risikerer å stanse arbeidet. Organisasjoner som ikke har kommet så langt med informasjonsklassifiseringen, mangler dermed full innsikt i hvor data lagres, hvem som eier den, hvordan tilgangen er regulert, samt om informasjonen er virksomhetskritisk. I tillegg er det en risiko for at domenekunnskap om dataene mangler eller er mangelfull i de delene av organisasjonen som forventes å gjennomføre det tekniske arbeidet, noe som gjør det vanskelig å arbeide med AI-spørsmål i virksomheten eller sammen med partnere. For å overvinne dette må arkitekturen muliggjøre desentralisering av data, men også et desentralisert eierskap til dataene som reduserer siloer og skaper større smidighet (agilitet) til å agere på endringer. En høyere modenhet og struktur rundt datahåndteringen muliggjør effektiv og sikker AI-bruk, skaper tillit og forutsetninger for å etterleve regelverk, samt muliggjør datadrevet beslutningstaking.

Tilgangen til og kvaliteten på data er også avgjørende for hvilke resultater som kan oppnås ved hjelp av AI. Organisasjoner som har tilstrekkelige mengder data av høy kvalitet, har bedre forutsetninger for å kunne trene modeller eller bruke teknologien til mer virksomhetsspesifikke brukstilfeller. Samtidig råder det en utbredt mangel på både datamengde og datakvalitet, noe som begrenser mulighetene for å realisere verdier ved hjelp av AI. De virksomhetene som har kommet lengst på reisen, uttrykker et tydelig behov for samhandling og å jobbe sammen i økosystemer. Å trene modeller på egne data i egen virksomhet blir vanskelig å gjøre godt nok uten enorme mengder data. Diskusjoner om felles bransje- eller sektorspesifikke modeller løftes frem som alternativer der lignende virksomheter kan gå sammen og dele data med hverandre.

“AI blir anledningen til å snakke om noe som ikke er så nytt ... Vi har for dårlige data og for lite data, og vi har ikke helt fått gehør for det. Dessuten har vi sensitive data, noe som også kompliserer det ... AI skaper bare virkelig verdi når man kan finne de dataene man trenger for å svare på de riktige spørsmålene”

– Digitaliseringsdirektør, svensk kommune

INFRASTRUKTUR

De skiftene i neste æra av AI som har blitt diskutert – forflytningen mot mer strategiske og virksomhetsnære anvendelser av teknologi med et større fokus på kontroll, valgfrihet og desentralisering – stiller krav til den underliggende strukturen for å muliggjøre dette. Detaljer som har blitt abstrahert bort gjennom årene mens vi har vært på en «skyreise», blir plutselig aktualisert på nytt, og dette stiller selvfølgelig også krav til kompetanse, prosesser og lederskap. I dette spørsmålet finnes det fortsatt store innsiktsgap. Mange organisasjoner ser fremover mot det nye, men har ennå ikke innsett fullt ut hva det vil kreve av underliggende infrastrukturelle kapabiliteter.

Når en stadig større del av logikk og beslutninger flyttes til kanten (edge) av virksomheten vår, endres selve infrastrukturen. Det fysiske miljøet med for eksempel butikker, fabrikker, kjøretøy og menneskelige interaksjoner blir en del av arkitekturen og stiller nye krav til virksomhetene. Datamengde, datakvalitet, beskyttelse og styring rundt dataflyt sammen med robust kommunikasjon blir strategiske nøkkelspørsmål. Dataarkitekturen må tilpasses, og regler for hva som skal forbli lokalt og hva som kan forlate stedet, må defineres.

“Fremtiden er en kollapset arkitektur som består av data og AI”

– CTO, privat sektor

Fordelingen av hvor vi utfører våre AI-kapabiliteter avgjør både opplevelse, risiko og kostnad. I scenarioer med strenge krav til ytelse, lav latens (kort forsinkelse) eller strenge krav til konfidensialitet, bør beslutningene tas ved kanten (edge). I andre tilfeller vil det være mer effektivt å håndtere beregning, kunnskap eller policyer sentralt. Trening og styring er som regel best sentralisert, der data og ressurser kan samordnes og kvalitetssikres. Hvordan AI-kapabiliteter vil bli utført, avhenger av individuelle forutsetninger og vil føre til ulike virksomhetsunike praktiske implementeringer. Beslutningsrammeverkene må veie konfidensialitet, total kostnad og tilgjengelighet opp mot kravene til ytelse og kvalitet.

I et agentbasert miljø der medarbeidere samhandler med ulike agenter, og der beregninger og beslutninger tas nærmere brukeren, vil virksomheter – i tillegg til data- og kommunikasjonsspørsmål – også måtte vurdere kapasitetsplanlegging. Et mer distribuert IT-miljø med dynamiske krav til infrastrukturen krever et nytt og bredere perspektiv på kapasitet. Agenter vil kreve rask tilgang til data eller systemer for å løse problemer med tidvis krevende arbeidsbelastninger, men krever også løpende verifisering av identitet og tilgangsregler. AI-klar infrastruktur handler ikke lenger bare om de store datasentrene, men om hver enkelt virksomhets kontorer, fabrikkgulv eller enheter.

70% av **AI-modne virksomheter** forventer at arbeidsbelastningen vil øke med mer enn **50%** de kommende 3–5 årene²

På samme måte som for datautfordringene, diskuteres samhandling også innen infrastrukturområdet i form av infrastrukturklynger. Ved å gå sammen kan virksomheter oppnå AI-kapabiliteter som er både mer virksomhetsnære og har høy kontroll og suverenitet, men som samtidig er skalerbare. Selv om samhandling er en viktig nøkkel på reisen, må virksomheter likevel vurdere hvilke kapabiliteter de selv må få på plass for ikke å sette seg fast i tekniske flaskehalser. Flaskehalser kan oppstå som en konsekvens av en omfattende digitalisering som over tid har innebåret snarveier, midlertidige løsninger eller kompromisser, og dermed har skapt en AI-infrastrukturgjeld. Denne gjelden omfatter ofte både infrastruktur, nettverk, sikkerhet og datahåndtering, og vanskeliggjør arbeidet med å utvikle virksomheten for morgendagen. En tydelig konsekvens er at virksomheter kjemper med store backlogger av arbeid som må prioriteres mot andre virksomhetsbehov. Dette kan også føre til at enheter i stedet begynner å bygge egne løsninger, noe som ytterligere forsterker fragmenteringen. Utover de tekniske flaskehalsene finnes også risikoen for at utviklingen begrenses av manglende kompetanse, utilstrekkelig forståelse av egne data og uklare prioriteringer av hvilke brukstilfeller infrastrukturen faktisk skal bære. For å realisere verdien av felles infrastrukturesatsinger kreves det derfor også en organisert kompetanseutvikling og styring der teknologi, dataforvaltning og virksomhet holdes sammen.

41% av svenske virksomheter oppgir at **teknisk gjeld** er det fremste hinderet for å omsette den digitale strategien til **konkrete resultater**⁸

SIKKERHET

Arbeidet med AI innebærer en oppbrytning av siloer for å muliggjøre dataflyt mellom systemer, funksjoner og organisasjoner. I praksis innebærer det en overgang fra vertikale løsninger til en horisontal lagarkitektur. Den horisontale plattformen skaper skalafordeler der hvert nye brukstilfelle kan settes sammen av etablerte lag, noe som både øker farten og senker kostnadene. For en virksomhet skaper det verdier som raskere tid-til-markedet, flere parallelle og en høyere andel vellykkede prosjekter, samt jevnere kvalitet i drift. Derimot stiller denne typen arkitektur helt nye krav til virksomhetens sikkerhetsarbeid. Tradisjonelt sett har vi også bygget sikkerhet i vertikale integrasjoner med robuste segmenteringer og kontroll over inn- og utflyt av data. Når siloer brytes opp og erstattes av en horisontal arkitektur, skapes eksponering mot en enorm mengde sikkerhetsutfordringer, og også sikkerhetsarkitekturen må tegnes på nytt med større fokus på integrerte og autonome sikkerhetskapabiliteter.

Sikkerhet i en virksomhet med distribuerte kunstige kapabiliteter bør bygges inn fra start. Et fragmentert miljø med mange nisjepregede og

spesialiserte løsninger driver frem høy kompleksitet, noe som også bidrar til et tydeligere skifte mot plattformer eller større løsningsblokker fremover. Sikkerhetsarbeidet bør bygges på en såkalt Zero Trust-basert modell, som innebærer at ingen brukere, tjenester, modeller eller agenter blir vist tillit uten at det alltid kreves verifisering. Tilgangshåndtering med kontinuerlig verifisering og observabilitet gjennom beslutningskjeder blir ekstremt viktig når AI-modeller blir stadig mer autonome og utfører oppgaver selvstendig i miljøet.

SUVERENITET

Med oppbrytningen av siloer og introduksjonen av kunstige anvendelser som kobles til mengder av ulike dataflyter og varierer hvor data håndteres, stilles det store krav til suverenitet. Suverenitetsdiskusjonen har vært tydelig preget av geopolitiske problemstillinger eller spørsmål om regeletterlevelse, men dreier seg i økende grad om det grunnleggende: kontroll over data. Økt oversikt og kontroll over data gir virksomheten forutsetninger for å kunne navigere og ta beslutninger i spørsmål som gjelder AI, skystrategier, sikkerhet og suverenitet. Snarere enn å ta utgangspunkt i eksterne faktorer og agere på dem, bør virksomheter ta utgangspunkt i seg selv med forståelse for egne datas krav til konfidensialitet, riktighet, tilgjengelighet og sporbarhet, og utforme strategier basert på dette.

Med utgangspunkt i hva som er mest virksomhetskritisk for hver enkelt virksomhet, kan suverenitetsspørsmålet brytes ned og håndteres på en mer pragmatisk måte. Både virksomhetskrav, behov og forutsetninger vil variere mellom virksomheter, noe som medfører en forflytning mot ulike varianter av hybride oppsett. Med en mer detaljert forståelse for hvilke krav som stilles til virksomhetens data, kan det egne IT-miljøet tilpasses for å imøtekomme kravene på en betydelig mer effektiv måte. De dataene, applikasjonene og systemene som er mest virksomhetskritiske og ikke kan stenges ned under noen omstendigheter, kan kreve en særskilt håndtering sammenlignet med de digitale eiendelene som ikke har samme nivå av kritikalitet. En infrastruktur som underbygger og muliggjør suverenitet har fokus på operasjonell fleksibilitet, økt kontroll og autonomi over data, oppfyller høye sikkerhetskrav, har mulighet til å isolere nettverk eller enheter, og som ofte muliggjør å kjøre sensitive arbeidsbelastninger lokalt (on-premise). Höga säkerhetskrav, har möjlighet att isolera nätverk eller enheter och som ofta möjliggör att kunna köra känsliga laster lokalt (on-premise).



TEKNISKE MULIGGJØRERE

DATA

Tilgang til og kvalitet på data er avgjørende for hvilke resultater som kan oppnås med AI.

- Informasjonsklassifisering basert på både sikkerhetskrav og datakvalitet
- Sikre effektiv og kontrollert tilgang til data for AI-modeller
- Samhandling og datadeling i økosystemer

INFRASTRUKTUR

En sikker og AI-klar infrastruktur er en grunnforutsetning for å kunne skape verdi med AI. Ny AI-teknologi stiller krav til en mer desentralisert infrastruktur.

- Retningslinjer og regler for hvor og hvordan data kan behandles
- Tilpasse dataarkitektur og kommunikasjonsnett til en mer distribuert driftsmodell
- Kapasitetsplanlegging for bruk av agentisk AI

SIKKERHET

Oppbrytning av siloer og et skifte fra vertikale til horisontale strukturer stiller nye krav til sikkerhetsarkitekturen.

- Sikkerhet må bygges inn fra start
- Fokus på integrerte og autonome sikkerhetskapabiliteter, for eksempel autonom segmentering
- Zero Trust-prinsipper, der all tilgang skal verifiseres

SUVERENITET

Suverenitet handler om kontroll over data for å kunne navigere i spørsmål som gjelder AI, sikkerhet eller skystrategier.

- Identifiser det som er mest virksomhetskritisk, og bygg en suverenitetsstrategi ut fra det
- Bryt ned problemstillingene og håndter det pragmatisk
- Bygg en infrastruktur som muliggjør suverenitet gjennom operasjonell fleksibilitet og kontroll over data

Kapabilitetene som kreves for å lykkes med reisen

De menneskelige, virksomhetsrelaterte og tekniske utfordringene og muliggjørerne som er diskutert, krever ulike typer kapabiliteter for å bli håndtert. I dette delkapittelet gis det konkrete råd, anbefalinger og fremgangsmåter som kan hjelpe på reisen. Disse baserer seg på Ciscos brede erfaring, ekspertise og spesifikke kapabiliteter knyttet til neste æra av AI.

“Vi må begynne med infrastrukturen, for den er bærende for alt annet. Først infrastrukturen og deretter data. Og å få samordnet de delene der ansvaret iblant ligger i ulike deler av organisasjonen”

– CIO, privat sektor

Veiledning for en verdiskapende AI-reise

AI-reisen går nå inn i en dypere og mer strukturert fase der fokus ligger på å skape tydelige verdier. For å lykkes kreves både sikre måter å bruke teknologien på, en tydelig struktur for hvordan AI skal integreres i virksomheten og en tilpasset operativ modell som støtter fremtidens AI, der tillit, kvalitet og suverenitet blir grunnpilarer.

TYDELIGE BRUKSTILFELLER ET VIKTIG GRUNNLAG FOR Å SKAPE VERDIER MED AI

AI skaper raskest og tydeligst nytte når den brukes til å løse konkrete virksomhetsproblemer. Ledende virksomheter har testet og eksperimentert med AI og går nå inn i en fase der reelle brukstilfeller ferdigstilles. Målsettingen er ofte vekst og å skape nye inntektskilder snarere enn effektivisering, men der kostnadsbesparelser og effektivitet følger som sekundære effekter i det lengre perspektivet (2–3 år). Den mest vellykkede veien fremover er dermed å ta utgangspunkt i tydelige brukstilfeller. Ved å skape en repeterbar innovasjonsevne der hver iterasjon ikke nødvendigvis fører til verdi, men der repeterbarheten og evnen til å trekke lærdom er en del av prosessen, skapes gode forutsetninger for å lykkes. Det er der AI-reisen begynner, og der verdien synliggjøres.

Suksessfaktor

Suksessfaktorer innebærer å fokusere på et begrenset antall prioriterte anvendelser der effekten kan måles i tydelige resultater, men også å drive brukstilfeller tverrfunksjonelt. Teknologi, virksomhet, juridisk og sikkerhet må samhandle fra start, ikke som separate spor. Det er først når AI anvendes på ordentlig i den daglige virksomheten, med tilgang til relevante data og tydelige styringsprinsipper, at effekten blir skalerbar. Organisasjoner som håndterer AI som en del av virksomhetsstrategien snarere enn som en eksperimentportefølje, får raskere verdi, lavere risiko og bedre styringsevne.

Virksomheters primære brukstilfeller²

Nå	Kommende 12 måneder	Kommende 2–3 år
Programvareutvikling med AI-assistenter og agenter som skriver, tester, feilsøker eller publiserer kode	Personlige assistenter og produktivitetsagenter. Ledende virksomheter ser også autonome agenter i virtuelle miljøer for tester eller simuleringer	Industrielle agenter og roboter som brukes innen logistikk, for å kontrollere droner eller selvkjørende biler

SKAP TILLIT GJENNOM KVALITET, SIKKERHET OG ETIKKBASERT AI

Å bruke AI for sikkerhet handler om å utnytte intelligente funksjoner for å identifisere, korrelere og utbedre cyberhendelser raskere enn vi mennesker rekker. Sikkerhet for AI handler derimot om å ta hensyn til to utfyllende perspektiver: trygghet og sikkerhet. Begge perspektivene må implementeres sammen, ellers blir risikoen bare flyttet.

Trygghet handler om å håndtere trusler som påvirker brukere, samfunnet og modellens etiske bruk, snarere enn tekniske sårbarheter. Dette inkluderer å forhindre at modellen genererer skadelig innhold som banneord, propaganda eller trakassering, samt å unngå at den oppmuntrer til selvskade eller økonomisk skade. I tillegg innebærer det å minimere risikoen for at modellen sprer feilaktig informasjon (såkalte hallusinasjoner), bidrar til sosial splittelse eller avviker fra oppgaven sin. Hva som anses som korrekt atferd varierer mellom virksomheter, regelverk og kulturelle sammenhenger, og endres dessuten over tid. Av disse grunnene må AI-systemene kunne styres dynamisk og fleksibelt ut fra både interne prinsipper og eksterne krav. I takt med at modellene blir mer autonome, vokser også behovet for å overvåke hvordan de resonnerer og trekker slutninger. Graden av innsyn må imidlertid tilpasses brukstilfellene, der enkelte anvendelser krever fullstendig åpenhet (transparens), mens andre bare trenger et visst mål av innsyn. Målet er å sikre at AI-modellen brukes på en ansvarlig og ufarlig måte for alle involverte parter. For å håndtere dette trengs tydelige beskyttelsesmekanismer som skjermer mot uønsket atferd og eksponering for risiko. Disse fungerer som innebygde «sikkerhetsbarrierer» (guardrails) som sørger for at AI-systemene holder seg innenfor de ønskede rammene.

Sikkerhet handler om å sikre at AI-systemene ikke blir utsatt for innbrudd, manipulasjon, tekniske trusler eller sårbarheter som kan kompromittere modellen, dens data eller den underliggende infrastrukturen. Disse truslene inkluderer angrep som innsetting av skadelige instruksjoner eller forgiftning av treningsdata for å manipulere modellens atferd eller læringsprosess. Det handler også om å beskytte mot tyveri av immateriell eiendom, som selve modellen eller dens treningsdata, samt å forhindre uautorisert tilgang. Til slutt omfatter sikkerhetsaspektet også beskyttelse mot kompromittering av infrastrukturen og å forhindre at modellen blir utilgjengelig gjennom for eksempel overbelastningsangrep.

Suksessfaktor

En viktig suksessfaktor utover de sikkerhetsskapabilitetene som allerede er nevnt, er observabilitet, noe som bør etterstrebes fra dag én for å unngå at virksomheten blir reaktiv. Aktiver og standardiser telemetri – altså fjernmåling med innsamling og analyse av data – i alle lag, fra nettverk og plattform til applikasjon, data og modell. Etabler en sløyfe der telemetri fører til innsikt som fører til tiltak. Da økes robustheten, og sikkerhetsnivået kan opprettholdes over tid.

BYGG EN AI-FABRIKK FOR MORGENDAGEN

Neste generasjons AI-fabrikk er basert på en plattformarkitektur med større, forhåndsintegrerte byggeblokker som er horisontalt skalerbar og har sikkerhet innebygd fra start. Den skal kunne tilrettelegge for nettverk av agenter som orkestrerer oppgaver, enten det er i datasentre, skyen eller ved kanten (edge). Kompleksitet driver risiko, noe som er en av de primære årsakene til at virksomheter beveger seg mot en plattformstrategi akkurat nå. Plattformen med større byggeblokker forenkler integrasjonsarbeidet for å spare tid og penger, samt minimere risiko. Morgendagens AI-fabrikk bygges dermed med færre, større og allerede integrerte komponenter som dekker nettverk, beregning, data, modellkjeder og drift. Det betyr ikke at virksomheter må låse seg til én enkelt leverandør, men det innebærer radikalt mindre egenintegrasjon.

Det store flertallet av fremtidens AI-arbeid vil skje nær brukeren. Dette drives av behovet for:

- Dataintegritet
- Sikkerhet
- Hastighet (lav latens/forsinkelse)
- Økonomi
- Regeletterlevelse

Dette krever nye løsninger skreddersydd for formålet, ofte i form av lokale enheter i nettverkets ytterkant – det som vanligvis kalles edge computing tilpasset distribuerte AI-anvendelser. Dette innebærer at infrastrukturkapabiliteter som kan utføre arbeidet, må flyttes ut nærmere både brukere og datakilder. Graden av distribuering av AI-kapabiliteter, og dermed infrastruktur, avhenger av kravene over og krever nye tekniske løsninger for å utnytte teknologien fullt ut uten å måtte gå på akkord med sikkerhet og ytelse.

Suksessfaktor

En suksessfaktor i arbeidet er en sentralisert styring med felles retningslinjer (policys) og regler. Selv om miljøet er distribuert, må det håndteres på en standardisert måte og styres med felles retningslinjer. For å både oppnå den verdiskapende effekten man søker, og lykkes med sikkerhetsarbeidet knyttet til dette, blir en sentralisert styring og ledelse kritisk for å muliggjøre en skalerbar infrastruktur for distribuert AI.

EN NY OPERATIV MODELL FOR DEN NYE AI-ÆRAEN

Den tekniske utviklingen blir en katalysator for endring og stiller krav til vår operasjonelle modell. En ny arkitektur krever en annen håndtering, ny kompetanse og tilpassede prosesser.

En målstyrt teknologi krever en mer målstyrt modell. Dagens arbeid handler mye om å beskrive våre arbeidsflyter og hvordan de ser ut, samt hvordan de får noe til å skje, og tilsvarende hva som skal skje hvis noe går galt. En fremtid med agentisk AI vil kreve en annen type modell som tar utgangspunkt i mål eller utfall. Snarere enn å definere en arbeidsflyt, defineres et utfall, og så skal det operative miljøet kunne realisere dette utfallet på en korrekt måte.

For å få en oversikt over behovet for tilpasning av den eksisterende modellen, kan virksomhetens ledelse ta utgangspunkt i en rekke trinn:

- Definere de nye kapabilitetene som vil kreves for å skape de forventede verdiene.
- Gjennomføre en GAP-analyse mellom den eksisterende operative modellen og de nye behovene.
- Definere de viktigste leveransene som den operative modellen skal levere.
- Vurdere om det er tilstrekkelig å justere og tilpasse den eksisterende modellen, eller om den må gjøres helt om ut fra de nye forutsetningene

Suksessfaktor

Suksessfaktorer er å bygge eller styrke evnen til å beskrive virksomhetens målbilder på en tydelig måte, men også å bygge inn sikkerhetsbarrierer (guardrails) som holder utfallene innenfor avtalte rammer. I tillegg må virksomheten definere tydelige nøkkeltall eller leveranser for den operative modellen som hjelper til med å utforme den..

INFRASTRUKTUR SOM MÖTER KRAV TIL SUVERENITET

I takt med at kravene til kontroll, autonomi og dataråderett øker, trenger virksomheter tekniske løsninger som ikke bare oppfyller regulatoriske krav, men som også muliggjør suverenitet i praksis. Dette innebærer behov for fysisk isolerte og konfigurerbare løsninger som kan driftes fullt ut i eget miljø. Europeiske virksomheter med behov for lokal kontroll, høy sikkerhet og begrenset skyeksponering krever tekniske kapabiliteter som omfatter alt fra nettverks- og datasenterinfrastruktur til samhandlingsplattformer og sikkerhetsløsninger. Disse løsningene må kunne driftes lokalt, oppdateres offline og tilpasses sektorspesifikke krav. Behovene drives av økende krav til digital suverenitet innen bransjer som energi, transport, offentlig sektor, finans og helse- og omsorgssektoren, der virksomhetskritiske data og systemer krever både geografisk og operativ selvstendighet, samt evne til å opprettholde drift selv under eksepsjonelle forhold.

“Vi trenger å ha større kontroll og unngå ensidige avhengigheter. Det er et tegn i tiden, men det må også balanseres. Hvordan bygger vi et effektivt økosystem der vi ikke mister innovasjon eller konkurransekraft samtidig som vi har fokus på disse spørsmålene?”

– Direktör, privat sektor

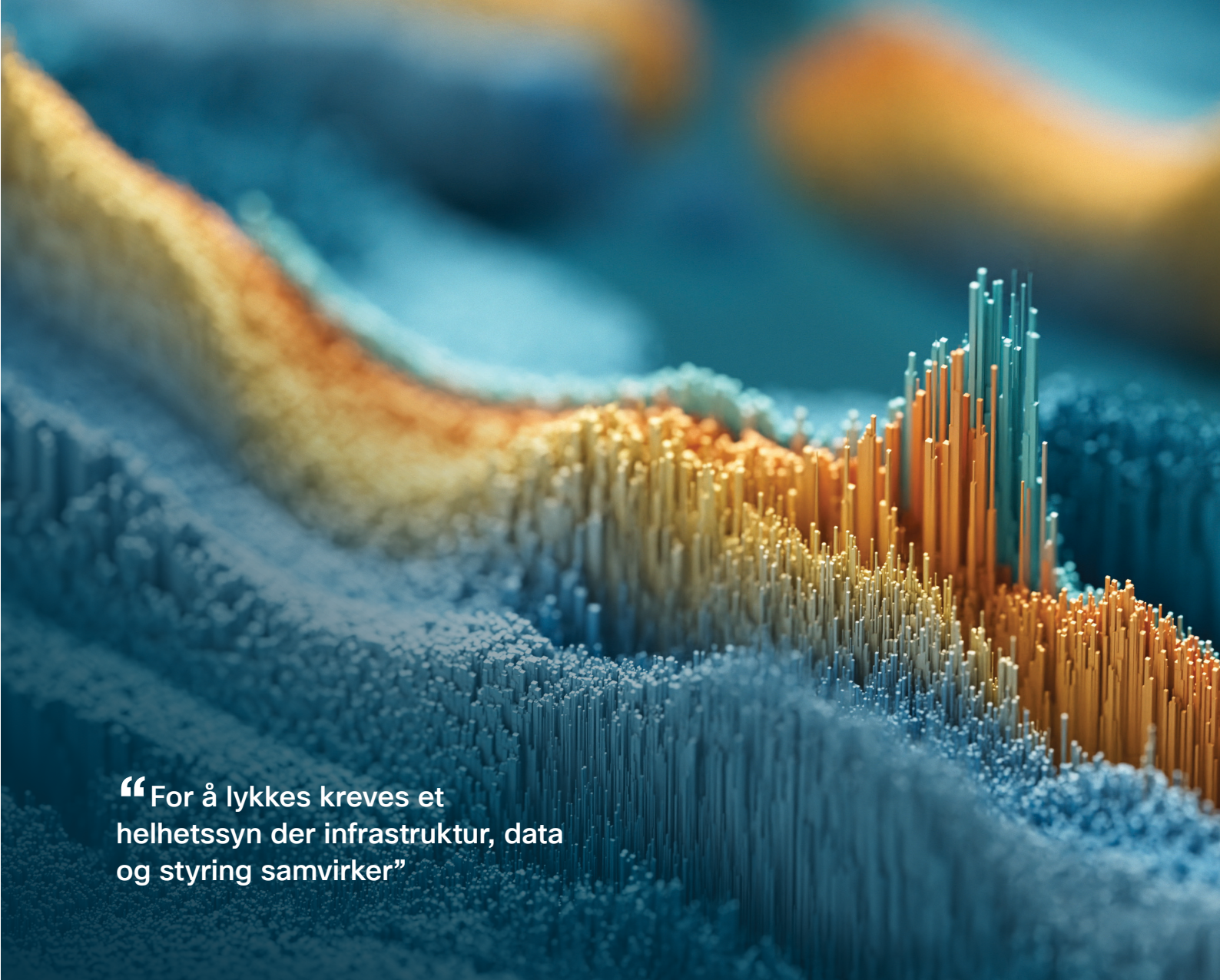
PRODUKTER I CISCO SOVEREIGN CRITICAL INFRASTRUCTURE

- Catalyst Center (DNA, UNX)
- SD-WAN / vManage
- Routing (inkl. IoT og MIG: NCS, ASR9k)
- Switching (Campus och IoT)
- Trådlöst (Campus, outdoor, IoT)
- Brannmurer
- Nexus
- UCS (Server) / Intersight (overvåking og orkestrering)
- Cisco Meeting Server (CMS)
- Webex Suite On-Prem (UCM)
- Contact Center
- Telefoner
- Videoutstyr

“Vi gir våre kunder mulighet til å kombinere Ciscos løsninger på en måte som imøtekommer deres krav til kontroll og suverenitet. Porteføljen støtter både generelle virksomhetsbehov og de høye kravene som følger med nasjonalt kritisk infrastruktur.”

– Thomas Brännström, CTO, Cisco Sverige

Samtlige produkter kan kjøres lokalt og i fysisk isolerte miljøer. Programvare kan oppdateres offline og administreres i kundens eget driftsmiljø.



“For å lykkes kreves et
helhetssyn der infrastruktur, data
og styring samvirker”

Fra teori til praksis: Cisco's rolle i AI-reisen

Å bygge en skalerbar og sikker AI-infrastruktur er en av de største utfordringene i den digitale omstillingen. AI endrer hvordan virksomheter arbeider, men teknologien stiller høye krav til data, sikkerhet og integrasjon. Mange organisasjoner setter seg fast i pilotprosjekter fordi de mangler en felles arkitektur som kan ta AI fra idé til produksjon. For å lykkes kreves et helhetssyn der infrastruktur, data og styring samvirker. AI skal ikke legges oppå eksisterende IT, men bygges inn i grunnmuren – med en robust, standardisert og automatisert arkitektur som støtter både dagens bruk og morgendagens modeller.

LØSNINGEN

Et moderne AI-økosystem bygger på arkitekturer som er testet, dokumentert og optimalisert som en helhet. Cisco tilbyr en modell som dekker hele reisen – fra strategi til drift – innen tre tydelige områder:

1

Rådgivning og behovsanalyse

Første steg er å forstå hvilken type AI-løsning som trengs. Gjennom konsultativ støtte hjelper Cisco organisasjoner med å analysere datamodenhet, identifisere forretningsnytte og definere riktig teknisk retning. Formålet er å skape klarhet: hvor AI skaper størst verdi, hvilke data som er mest kritiske og hvordan infrastrukturen bør bygges for å møte krav til sikkerhet og etterlevelse.

2

Arkitektur og teknisk løsning

For å møte kravene i neste æra av AI, tilbyr Cisco en sikker AI-klar infrastruktur som spenner fra AI-forberedte datasentre til fremtidssikrede arbeidsplasser og digital resiliens i nettverk og sikkerhet. Gjennom en sammenhengende arkitektur med forhåndsvaliderte byggeblokker kan organisasjoner bygge og skalere AI-løsninger i hele sitt miljø, fra datasenter og sky til kanten (edge). Når behovene er tydelige, brukes Cisco Validated Designs (CVD) – forhåndsvaliderte og dokumenterte arkitekturer som beskriver beste praksis for AI-infrastruktur. CVD-løsninger er testet i reelle miljøer og omfatter hele kjeden:

- **Sikkerhet** – Zero Trust-basert beskyttelse med identitetshåndtering, segmentering og autonome kapabiliteter for å detektere og beskytte mot trusler i hele AI-miljøet.
- **Observabilitet** – sammenhengende telemetri og sanntidsinnsyn som gjør det enkelt å overvåke, feilsøke og optimalisere alle AI-arbeidsbelastninger.
- **Compute** – GPU-optimaliserte plattformer for trening og inferens, med støtte for NVIDIA Enterprise.
- **Nettverk** – segmenterte nettverk med høy ytelse og innebygde sikkerhetslag.
- **Orkestrering** – containerbaserte plattformer, som Red Hat OpenShift, for skalerbar modellhåndtering.
- **Data** – integrerte partnerskap med Vast, NetApp og Hitachi for sikker datalagring og flytkontroll.

Cisco's plattform for sikker AI-klar infrastruktur og CVD reduserer integrasjonsrisiko, forkorter tiden til utrulling og gir forutsigbar ytelse og sikkerhet. Arkitekturen støtter hele AI-livssyklusen – fra bruk ved kanten (edge) til storskala modelltrening – og er bygget for resiliens, observabilitet og effektiv ressursbruk.

3

Implementering og integrasjon

Gjennomføringen er avgjørende. Cisco og sertifiserte partnere sikrer en rask og sikker installasjon, med sentralisert styring og automatisert livssyklusstyring. Ved å integrere AI-løsningene med eksisterende IT-prosesser blir drift og support en naturlig del av virksomheten. Energieffektivitet og ytelsesoptimalisering er innebygde mål. AI-arbeidsbelastninger krever betydelig datakraft, og infrastrukturen skal kunne skaleres uten at energiforbruket øker uforholdsmessig mye.

HELHETSPERSPEKTIVET

AI-infrastruktur handler ikke bare om teknologi – men om styring og sikkerhet. Zero Trust-prinsipper sikrer at hver bruker, enhet og applikasjon verifiseres før tilgang gis. Segmenterte nettverk, ende-til-ende-kryptering og sanntidsovervåking beskytter både data og modeller. En annen nøkkel er livssyklus håndtering. AI-modeller krever oppdatering, re-trening og kontinuerlig validering. Gjennom standardiserte prosesser kan dette automatiseres og kontrolleres, noe som sparer tid og sikrer kvalitet over tid..

SAMMENDRAG

Den nye generasjonens AI-infrastruktur krever at organisasjoner legger komplekse, manuelle prosjekter bak seg. Ved å kombinere rådgivning, standardisert arkitektur og strukturert implementering kan virksomheter raskt gå fra idé til verdi. Med Cisco Validated Designs som grunnlag får organisasjoner en plattform som er:

- **Sikker** – Zero Trust med helhetlig innsikt og kontroll.
- **Skalerbar** – klar til å vokse i takt med nye behov.
- **Effektiv** – optimalisert for ytelse, energi og drift.
- **Håndterbar** – sentralisert, forutsigbar og livssyklusstyrt.

Dette helhetsgrepet gjør det mulig å realisere AI på ordentlig – raskt, sikkert og bærekraftig.

Silker **AI-klar** infrastruktur

AI-klare
datasentre

Fremtidssikrede
arbeidsplasser

Digital resiliens

<<<<<<<<< Akselereres med CISCO AI >>>>>>>>>

Konkrete sluttanbefalinger til beslutningstakere

I tillegg til anbefalingene som har blitt presentert fortløpende for mennesker, virksomhet og teknologi, ønsker rapporten å gi leseren noen avsluttende anbefalinger som oppsummerer noen av de viktigste forutsetningene for å lykkes med den transformative og verdiskapende AI-reisen.



ET STRATEGISK OG PROSESSFOKUSERT ARBEID

- Ta neste steg fra den ustrukturerte og utforskende fasen av AI-reisen
- Utform neste steg basert på virksomhetens strategi og mål, og etterstrebe å agere som en nyttestyrkt virksomhet
- Sett tydelige prioriteringer og forventninger basert på virksomhetsforankrede brukstilfeller



INVESTER TIDLIG I SIKKER OG AI-KLAR INFRASTRUKTUR

- Målbildet bør være en sikker og skalerbar AI-infrastruktur
- Bygg suksessivt og parallelt med innføring, med fokus på å kunne skalere pågående initiativer
- Prioriter suverenitet, operasjonell fleksibilitet og unngå innelåsing



SE PÅ DATA SOM EN NY DISIPLIN I ORGANISASJONEN

- Etterstrebe demokratisert datatilgang og oppbrytning av datasiloer
- Prioriter sikker og smidig tilgang til data av god kvalitet
- Etabler en plattformstrategi for datahåndtering som sikrer råderett over egne data



DRIV TRANSFORMASJON FOR Å OPPNÅ TRANSFORMATIVE VERDIER

- Tilrettelegg for tverrfunksjonell verdiskaping i organisasjonen
- Sikre nødvendige kapabiliteter og kompetanse, og innfør nye roller ved behov. Tydeliggjør beslutningsskjeder og mandater for raskere prosesser
- Modifiser eller innfør en ny operativ modell tilpasset AI dersom det kreves



BALANSER INNOVASJON MED SIKKERHET

- Skap tillit gjennom tydelig overvåking, styring og beskyttelsesmekanismer for AI
- Etabler en ny forvaltningsmodell som er tilpasset nettverk av AI-agenter, samt rutiner for klassifisering og tilgangsstyring
- Sikre at det finnes tydelige retningslinjer (policies) for AI som støtter beslutningstaking

Sluttord

Kunstig intelligens har gjort et tydelig inntog i svenske (og norske) virksomheter. I dag er det i første rekke individet som drar nytte av produktivetsgevinstene, samtidig som mange er usikre på hvilken verdi AI skaper på organisasjonsnivå. De fleste virksomheter har forlatt den tidlige eksperimentfasen og jobber nå mer systematisk med å integrere teknologien for å skape reelle virksomhetsverdier. Samtidig står neste generasjon AI allerede rundt hjørnet: mer autonome systemer, mer virksomhetsnære anvendelser og en høyere grad av integrasjon i kjerneprosesser. Denne forflytningen stiller helt nye krav til virksomheter som ønsker å skape verdi på en bærekraftig og skalerbar måte.

Mange svenske (og norske) virksomheter er fortsatt forventningsstyrte. Et teknologidrevet fokus og reaktive satsinger fører ofte til punktinnsetser og begrenset nytte. Det er i stedet de nyttestyrte virksomhetene som lykkes best både nå og fremover. De jobber holistisk og balanserer strategi, infrastruktur, data, styring, mennesker og kultur. De veier sammen suverenitet, fart, innovasjon og sikkerhet, og bygger suksessivt de underliggende kapabilitetene som kreves for reell transformasjon.

Så for å oppsummere handler suksess om å styrke de grunnleggende kapabilitetene. Virksomheter må gå fra eksperimenter til en strategisk og prosessdrevet arbeidsmåte, investere tidlig i sikker og skalerbar AI-infrastruktur og etablere data som en egen disiplin. De må drive transformasjonen tverrfunksjonelt, bygge riktig kompetanse og sikre at styring og sikkerhet utvikles i takt med bruken.

Det er denne balansen som skaper helhet og legger grunnlaget for en langsiktig verdiskaping med AI.

Referanseliste

1. BCG & Harvard's Digital Data Design Institute (2023). Navigating the Jagged Technological Frontier: Field Experimental Evidence of the Effects of AI on Knowledge Worker Productivity and Quality. https://www.hbs.edu/ris/Publication%20Files/24-013_d9b45b68-9e74-42d6-a1c6-c72fb70c7282.pdf
2. Cisco (2025). Realizing the Value of AI: Cisco AI Readiness Index 2025. https://www.cisco.com/c/dam/m/en_us/solutions/ai/readiness-index/2025-m10/documents/cisco-ai-readiness-index-2025-realizing-the-value-of-ai.pdf
3. European Commission (2025). Denmark 2025 Digital Decade Country Report. <https://digital-strategy.ec.europa.eu/en/factpages/denmark-2025-digital-decade-country-report>
4. European Commission (2025). Finland 2025 Digital Decade Country Report. <https://digital-strategy.ec.europa.eu/en/factpages/finland-2025-digital-decade-country-report>
5. European Commission (2025). Sweden 2025 Digital Decade Country Report. <https://digital-strategy.ec.europa.eu/en/factpages/sweden-2025-digital-decade-country-report>
6. McKinsey (2025). A new operating model for a new world. <https://www.mckinsey.com/capabilities/people-and-organizational-performance/our-insights/a-new-operating-model-for-a-new-world>
7. MIT (2025). The GenAI Divide. State of AI in Business 2025. https://mlq.ai/media/quarterly_decks/v0.1_State_of_AI_in_Business_2025_Report.pdf
8. Radar (2025). Radar Research 2025. Data tillgänglig på begäran.
9. Radar (2025). Svensk cybersäkerhet 2025. <https://hub.radargrp.com/content/svensk-cybersakerhet-2025>

Foton

Omslag: iStockphoto, hqrloveq

Sid 4: Unsplash, Charles Etoroma

Sid 18–19: Unsplash, Fredrik Ohlander

Sid 45: iStockphoto, DKosig

