Innspill fra Cisco Norge AS til regjeringens Digitaliserings-strategi

Digitaliseringsstrategien bør knyttes til EUs digitaliseringspolitikk

- **Cisco ønsker en strategi som utnytter potensialet i EUs digitaliseringspolitikk.** Den digitale strategien må koordineres til pågående EU-politiske spørsmål exempelvis NIS2 og andre som vil ha innvirkning på cybersikkerhetsspørsmålene. Strategien må ha konkrete resultatmål for å gjøre det mulig å følge opp og evaluere. Dette bør være en viktig del digitaliseringsstrategien.

Sikre behovet for teknisk kompetanse

- **Det bør igangsettes et målrettet initiativ fokusert på digital kompetanse og cybersikkerhet rettet mot offentlig sektor**. Utfordringen med mangel både på digital kompetanse og spesifikt på Cyber-sikkerhet er enorm og dette skaper sårbarhet i seg selv. Det er et sterkt behov for å kartlegge og møte etterspørselen etter ferdigheter innen Cyber-sikkerhet, og dette bør gjøres samarbeid med industri og høyere utdanning.
- **Det bør igangsettes et eget initiativ innen videreutdanning i Industri og kraftbransjen på Digital kompetanse**. I dag er det et gap i kompetanse og forståelse mellom de som håndeterer IT-systemer og OT-systemer (prosess-industri etc). Dette skaper stor sårbarhet for Industrielle systemer.
- **Mangel på Digital Kompetanse.** Digitalisering innen all industri og kraftbransje krever at all høyere utdanning gis opplæring i digitalisering og cyber sikkerhet, ikke bare dedikerte IT-bachelor. Slik det i stor grad er i dag, som igjen skaper behov for en stor grad av videreutdanning når studenter kommer ut i arbeidslivet. Dette er ikke hensyntatt idag.
- **Det finnes mange private utdanninger som alternativer til de offentlige.** Vi i Cisco har et globalt verdensledende opplæringsprogram og er tilgjengelig lokalt på 12 000 steder rundt om i verden og tilbyr gratis kurs og programmer innen IT Stort potensial i å bruke private initiativ.

Digital trygghet og beredskap

- Både globalt og såvel i Norge er mye av en nasjons kritiske infrastruktur i hendene på privat sektor, og samarbeid gir selskaper og offentlige enheter en god løsning for å forstå og beskytte de gjensidige avhengighetene som ikke bare er avgjørende for en nasjons sikkerhet, men også for innbyggernes helse og velvære. Idag eksisterer det ikke dette samarbeidet på en god nok måte.

- Vi mener at den digitale strategien bør adressere utfordringen rundt synlighet inn i digitale avhengigheter og mangel på synlighet i disse avhengighetene.
- Den bør adressere samarbeid på tvers av sektorer som utgjør totalforsvaret av Norge. Vår observasjon er at dette idag ikke er godt nok implementert.
- Strategien bør adressere fysisk infrastruktur og dens robusthet – og innunder her spesielt kritiske områder.
- Den bør adressere mangel på kompetanse innen offentlig sektor, på anskaffelses-siden og bruken av dette. Dette gjelder grunnleggende digital kompetanse, men også innen spesifikke områder som Cyber-sikkerhet, infrastruktur, OT, og bør inkludere videreutdanning.
- **Regulering og krav rundt bruken av fiber infrastruktur i lys av de mest kritiske infrastrukturer.** Det vil være hensiktsmessig at kritisk infrastruktur i krise kan bruke hverandre som bærere ved utfall. I dag kan konkurransefortrinn hindre samarbeid.
- **Geopolitisk usikkerhet.** Vi ser et større fokus på robusthet i infrastruktur etter erfaring fra Ukraina, samtidig som operatører ser at dette må løses tverr-sektorielt (på tvers av kritisk infrastruktur). Diskusjoner rundt behovet for å fungere autonomt om deler av kommunikasjons infrastruktur blir slått ut.

<u>Tildel ressurser og skape partnerskap med teknologiindustrien</u>

- **Den geo-politiske situasjonen har styrket partnerskap mellom privat næringsliv og myndigheter.** Disse offentlig-private partnerskapene gjør det mulig for begge parter å utveksle viktig informasjon, ressurser og ekspertise, og er også nødvendig for å lage risikostyringsplaner/beredskaps-planer og gjennomføre responsøvelser for å sikre beredskap mot potensielle trusler. Offentlige etater har unik kjernekompetanse som utfyller styrker i privat sektor. Vi mener derfor det er av ytterste viktighet at dette samarbeidet blir konkretisert i **privat-offentlig råd for implementering av digital strategi og oppfølging**. Dette rådet må ha konkrete mål og mulighet for å følge opp disse målene. Dette bør også være fokusert på konkrete områder, og ikke bredt utvalg/råd.
- **Vi foreslrå etablering av et tverr-sektorielt koordinerende råd som samler eiere og operatører av kritisk infrastruktur for å ta opp og lage konkret planer rundt grunnleggende spørsmål som (og dette er noen eksempler):**

a) Hvordan dele informasjon mellom sektorer. Kartlegge barrierer for informasjonsdeling.
b) Hvordan gjensidig avhengighet mellom sektorer påvirker reaksjoner på nødssituasjoner.
c) Fysisk infrastruktur og robusthet – Gi innsikt, synlighet og avdekke behov for evnt utbygging for å skape mer redudans på lag 1.
d) Peering: Gi innsikt, synlighet og forståelse av om peering innad i Norge og eksternt er tilstrekkelig for de mest kritiske tjenester.
e) Kritisk infrastruktur er avhengig av autorative kilder til presis tid for synkronisering, GPS og satelitt. I Ukraina førte «jamming» av klokke til en stor trussel for sikkerhet og angrep. Dette er arbeid som må koordineres; hvordan alternative kilder og sikring av dette skal gjøres.
f) Hvorvidt myndighetene har de riktige anrops-listene og kontaktpunktene på tvers av infrastrukturer for å gi en koordinert respons på fysiske trusler eller cybertrusler

Styrke informasjon og cybersikkerhet

- **Dagens komplekse cyberutfordringer krever godt samarbeid mellom politikere og næringsliv.** Bedriftenes rolle i å sikre Norges cybermiljø er helt avgjørende. Ønsket om et sterkt økosystem for cybersikkerhet som samler aktører i offentlig og privat sektor er etterspurt. Cybersikkerhet er en av de største utfordringene bedrifter står overfor i dag. Selskaper, stater og myndigheter opererer i et globalt marked og i et totalt tilkoblet miljø. Med det følger nye trusler og krav til sikkerhet og personvern som må adresseres.
- **Dra nytte av den verdensledende ekspertisen som er tilgjengelig i Norge.** Det kreves omfattende offentlige investeringer for å sikre cybersikkerhet i Norge.
- **Utvid cybersikkerhetsutdanning:** Cybersikkerhetsutdanning må styrkes som et eget fagområde for å møte behovene nå og i fremtiden. Cybersikkerhet bør integreres i den grunnleggende digitale kunnskapen.
- **Økt kompetanse i offentlig sektor:** Øke kompetansen om cybersikkerhet i offentlig sektor. Cybersikkerhet bør integreres i kompetanseheving i offentlig sektor.
- **Det er viktig med politisk enighet rundt regelverk og standardisering** – gjerne på et grenseoverskridende nivå.

Teknisk politikk uten unødvendige hindringer

- **Gjennomgå gjeldende lov.** Sette opp et digitaliseringsforberedelse med oppgave å gjennomgå gjeldende lov og foreslå endringer fortløpende for å sikre at lovverket ikke hindrer eller unødvendig vanskeliggjør digitalisering
- **Sørge for at lovverket følger med den raske teknologiutviklingen.** Etablere en funksjon som er ansvarlig for at all ny lovgivning som presenteres er "digital som standard". All ny lovgivning må følges av en konsekvensanalyse der effektene på digitaliseringen er undersøkt og det må sikres at nye lover ikke er til ulempe for bruken av digitale tjenester og teknologier.

Teknologi for bærekraftig utvikling

- Det er gledelig å se at bærekraftsmålene er en enorm pådriver for digitalisering av industrien, også i olje og gass.
- Kraftbransjen må også digitaliseres mye mer skal de kunne operere mer effektivt enn i dag. Digitaliseringen som kraftbransjen nå må stå i for å levere mer kraft ihht bærekraftsmål
- Totalt sett har digital innovasjon et enormt potensial for å øke bærekraften. Felles næringsprosjekter i den grønne omstillingen bør prioriteres.
- Det kreves et tydelig og langsiktig regelverk som støtter bærekraftig utvikling.

Nye teknologier

- Kommersialiser og distribuer fremvoksende teknologier som er avgjørende for en voksende og motstandsdyktig økonomi: sørg for planer for å støtte kommersialisering og distribusjon av fremvoksende teknologier, fra AI og Quantum til EV.

- Støtte et blomstrende digitalt og AI-etisk økosystem for å muliggjøre bedre styring og regulering: ved å etablere nye tekniske arbeidsgrupper. Kunstig intelligens underbygget av et system med AI-etikk, styring og regulering.

Cisco vill bidra i det fortsatta arbetet med den digitala strategin

- Som et globalt selskap er vi engasjert i å rådgi myndigheter over hele verden. Eksempel fra Sverige, Danmark og Nederland, hvor Cisco er representert i råd og utvalg satt ned av myndighetene. Vi bidrar med vår kompetanse, og vi kan som global aktør dele det vi ser av gode initiativ.
- Cisco ønsker å være en aktiv partner for regjeringen i prosessen med å forme den digitale strategien for Norge på områder som: cyber-sikkerhet, kritisk infrastruktur og økosystem rundt data, grønn og digital transformasjon av næringsliv og offentlig tjenester, data suverenitet og digitale ferdigheter (NetAcad).
- Cisco ønsker også å være en aktiv partner for implementasjons- og oppfølgingsprosessen av strategien innenfor våre kompetanseområder.