IKT Norge

NOTAT

TIL: Næringsminister Jan Christian Vestre

Oct 20, 2022

FRA: IKT-Norge

INITIATIV OM NORSK CYBERPAKT

Vi viser til vårt initiativ om en norsk "cyberpakt" etter dansk modell og kommende møte med statsråden 25.10.. Dette notatet er et forsøk på å i noen grad konkretisere og operasjonalisere vårt initiativ.

Bakgrunnen for vårt initiativ

IKT-Norge har i lang tid, men spesielt det siste året, hatt et betydelig engasjement knyttet til cybersikkerhet på alle områder i Norge. Bakgrunnen for dette er for det første en rekke angrep på norske bedrifter, kommuner og offentlige etater. For det andre at det politiske ansvaret for cybersikkerhet i Norge framstår for oss som for fragmentert og utydelig. "Alle" vet, men "ingen" tar overordnet ansvar.
Vi understreker at det siste ikke er en kritikk rettet mot noen spesiell statsråd, og aller minst næringsministeren. Og for det tredje en rekke kritiske rapporter knyttet til cybersikkerhet m.m. fra Riksrevisjonen, senest rettet mot Forsvaret.

Samtidig er det etter vårt syn enkeltnæringer som har lykkes godt i sitt arbeid med datasikkerhet, ikke minst finansnæringen. Det er et arbeid og en arbeidsform som bør kunne overføres til andre sektorer/næringer.

Vårt initiativ kan derfor oppsummeres i tre formål. 1) Tydeliggjøre det politiske ansvaret., 2) Bedre samarbeidet mellom myndigheten og næringslivet om cybersikkerhet og 3) Bedre (og mer samlet) informasjon til innbyggere og bedrifter om datasikkerhet.

Vi understreker igjen at ikke alt dette pt er næringsministerens konstitusjonelle ansvar, men skal vi styrke arbeidet på dette området må vi etter vårt syn ut av "silotekningen" og samarbeide bedre på tvers av sektorer og formelle ansvarsområder.

Vi mener også at et slikt samarbeid eller pakt ikke ensidig skal bety "merbelastning" på det offentlige, men at det også kan innebære at det stilles strengere krav til næringslivet knyttet til rutiner og standarder når det gjelder datasikkerhet, f.eks. sertifiseringsordninger etter modell av den britiske cyber essential. Vi er også kjent med at det er lignende initiativ fra DNV og Gjensidige i Norge.
Det kan også være at næringsliv og akademia i samarbeid etablerer et samarbeid for å utdanne eller videreutdanne flere med relevant cyberkompetanse.

Kort om den danske "cybersikkerhetspagt"
Med bakgrunn i den økte sikkerhetstrusselen som følge av Russlands invasjon av Ukraina og det faktum at kun 40 prosent av små og mellomstore danske virksomheter har tilstrekkelig digitalt sikkerhetsnivå i forhold til egen risikoprofil, har det danske Ervervsministeriet (tilsvarende nærings- og handelsdepartementet) inngått en avtale/cybersikkerhetspakt mellom regjeringen og interesseorganisasjoner for det private næringsliv i Danmark, tilsvarende bl.a. NHO, Norsk Industri, Finans Norge, IKT-Norge, Abelia, SMB Norge, Tekna, Handel og Kontor, oversatt til norske forhold.

Målsettingen for arbeidet er at Danmark skal ha Europas mest digitalt sikre små- og mellomstore virksomheter. Partene har forpliktet hverandre på å igangsette og koordinere innsats for å styrke cybersikkerheten i danske private virksomheter, utveksle data og erfaring om digitale trusler og samarbeide om bedre synergieffekter i arbeidet med å utvikle et bedre cyberforsvar.

I første omgang skal det utvikles et bransjerettet program for styrke cybersikkerheten i enkelte utvalgte og utsatte bransjer. Konkret vil dette handle om å samarbeide om tekniske løsninger, datadeling, trening på å håndtere angrep og kompetanseoppbygging internt i bedriftene.

Hvordan kan en norsk modell se ut?
Vi mener at en norsk modell både kan og bør ta utgangspunkt i den danske. Det er etter vårt syn viktig at vi gjør noen funksjonelle enkeltgrep for å styrke datasikkerheten i norske bedrifter, heller enn å lage store planer og nye omfattende strategier.

Vi foreslår i første omgang fire konkrete tiltak:

1) Opprette en møteplass mellom NFD og berørte/interesserte nærings- og interesseorganisasjoner etter modell av referansegruppen for grønn finans.
2) Utvikle bransjeprogram etter dansk modell.
3) Gjennomføre 1-2 større øvelser per år mellom myndigheter og næringsaktører.
4) Opprette en portal tilsvarende sikkerdigital.dk

Møteplass mellom NFD og berørte nærings- og interesseorganisasjoner:
Etter initiativ - ikke helt ulikt dette - fra NHO, Finans Norge og Rederiforbundet nedsatte daværende regjering våren 2021 en referansegruppe for grønn finans, ledet av Finansdepartementet.. Dette arbeidet er videreført av dagens regjering. Referansegruppen består av representanter for myndigheter, nærings- og interesseorganisasjoner og akademia og er et forum for informasjonsutveksling, identifisering av forhold av særlig betydning og nyttiggjøring av kunnskap og innsikt. Vi mener en tilsvarende modell kan danne grunnlaget for arbeidet mellom myndigheter og nærings- og interesseorganisasjoner om cybersikkerhet. Listen av organisasjoner vi har pekt på i beskrivelsen av den danske modellen, kan danne et grunnlag, men er ikke uttømmende. Det vil være naturlig at Digital Norway som retter seg spesielt mot små og mellomstore bedrifter deltar, og det kan være en idé å koble på Center for Cyber and Information Security ved NTNU Gjøvik i et slikt arbeid.

Hvordan et slikt samarbeidsorgan skal organiseres og hva det skal gjøre eller diskutere er vi svært åpne for å diskutere. Aktuelle problemstillinger kan f.eks. være:

- Kompetanse. Hva trenger næringslivet og hvordan får vi det til?
- Informasjon og intelligence. Hvordan får vi til rask nok spredning av relevant informasjon og til den/de riktige mottakerne?
- Tydelig og effektiv ansvarsdeling. Hvem har ansvar for hva når?
- Sikkerhetskultur- og forståelse. Hvordan etablere vi det?
- Prioritering av offentlige midler i trange økonomiske tider. Hvordan får vi best effekt av hver offentlig krone? Er det datasikkerhetsprosjekter eller modeller det offentlige og private kan samarbeide (bedre) om?

Punktene over er på ingen måte uttømmende.

Utvikle bransjeprogram
Vi mener det er en god idé at et første konkret mål er å utarbeide bransjeprogram for særlig utsatte grupper. Bransjeprogrammene bør inneholde konkrete tiltak for hvordan cybersikkerheten kan styrkes innenfor spesielt utsatte næringer og om nødvendig følges opp med forslag til bevilgning ifbm RNB 2023 eller NB 2024 avhengig av framdrift og konkretisering. I Nkoms nylig framlagte "Nasjonalt digitalt risikobilde"

utpekes teknologibedrifter som en av tre spesielt utsatte områder (sammen med forskning og utvikling og offentlige forvaltningsorganer) for hyppige cyberangrep. Det kan også være andre, eller mer spesifikke næringer enn "teknologibedrifter" som bør prioriteres.

Gjennomføre en til to større "nasjonale" øvelser per år
Vi mener at det er avgjørende viktig at det øves mer for å forhindre dataangrep på kritiske infrastruktur eller viktig data. Vi mener derfor at det bør gjennomføres en til to større koordinerte øvelser på tvers av myndigheter og næringsliv i året. Gitt ressurssituasjonen som vil måtte påregnes for å få det så realistisk som mulig, er det mest formålstjenlig å starte med en årlig øvelse og eventuelt trappe opp senere. Vi foreslår at det blir en oppgave for en slik referansegruppe som vi foreslår i punkt 1, å konkretisere hvordan en slik øvelse blir mest mulig reell og hensiktsmessig, men det er viktig at det skjer på tvers av bransjer og at det både er store og små med. Det kan f.eks. tenkes at en slik øvelse kan gjøres med utgangspunkt i det som allerede skjer i store samfunnskritiske aktører som Telenor.

Opprette en portal tilsvarende sikkerdigital.dk
Vi foreslår å opprette en nettportal tilsvarende den danske sikkerdigital dk hvor all informasjon om digital sikkerhet samles på ett sted - både til borgere, bedrifter og offentlige organ og etater. Det finnes informasjon om dette i Norge i dag, bl.a. er norsis.no kanskje det nærmereste vi kommer den danske portalen, men igjen er det fragmentert og vanskelig å finne. På samme måte som den danske, bør dette være et samarbeidsprosjekt mellom ulike offentlige organ som har en eller flere roller knyttet til digital sikkerhet. I tillegg bør en slik portal være en felles digital inngang for å melde fra om digitale sikkerhetshendelser til offentlige myndigheter. I den forbindelse mener vi også at det bør innføres en obligatorisk meldeplikt for slike hendelser.

Vi mener også at det kan være en god idé å opprette et "Center of Excellence" på forskning innen cybersikkerhet. Om det skal være en del av NFDs portefølje når det gjelder forskning, eller om det er mer naturlig å legge det til et annet departement er vi åpne for å diskutere, men det harmonerer godt med formulering i regjeringsplattformen om at regjeringen vil *"utvide satsinga på framifrå forskings- og utdanningsmiljø og etablere nye forskingsmiljø i internasjonal toppklasse knytt til næringsklynger"*.

Hensikten med et slikt senter bør etter vårt syn både være å kraftsamle den kompetansen som finnes i Norge (gjerne i et virtuelt nettverk), tiltrekke oss kompetanse fra øvrige nordiske land (det kan f.eks. være et konkret oppfølgingspunkt fra vårt felles arrangement i Sverige i mai i år) og å utvikle egne sertifiseringløsninger rettet mot

selskaper og organisasjoner. Vi vil også peke på utfordringer knyttet til felles sikkerhetsklarering av personell og redundante løsninger og utfordringer knyttet til sikkerhetsloven, for å gå til et bedre samarbeid om cybersikkerhet, og da spesielt for næringslivet, over landegrensene i Norden. De globale sikkerhetsutfordringene har hetter vårt syn aktualisert denne problemstillingen ytterligere.

Vi understreker igjen at dette notatet ikke er uttømmende når det gjelder tiltak og innhold i et samarbeid mellom myndigheter og næringsliv aka. "cybersikkerhetspakt". IKT-Norge har bl.a. etablert et et eget cybersikkerhetsforum. Dette forumet skal ha møte førstkommende fredag, med over 50 påmeldte deltakere fra våre medlemsbedrifter (og hvor bl.a. Forsvaret har bedt om å få være observatør). På møtet skal vi også diskutere konkrete tiltak som kan supplere det som vi allerede har skissert over. Vi tar med oss innspill fra dette møtet til vårt møte tirsdag 25.10.