Vår saksbehandler
Lene B. Kaland
+47 67864289, 05154289
lene.kaland@nsm.stat.no

Vår dato
2010-03-26

Vår referanse
2009/01235-008/NSM/430

Tidligere dato
2010-01-28

Tidligere referanse
2009/01235-003/NSM/430

Til
Forsvarsdepartementet
v/avdelingsdirektør Annette Tjaberg

Kopi til
Justis- og politidepartementet

Internt

Intern kopi

# Forslag til nasjonal strategi for cybersikkerhet - økonomiske og administrative konsekvenser

Ved vurderingen av de økonomiske og administrative konsekvenser av gjennomføringen av forslaget til strategi er det viktig å fremholde at de enkelte delstrategier i mange tilfeller tar utgangspunkt i og bygger på eksisterende ordninger og tiltak som er fremkommet over lang tid. Gjennom disse er en stor del av de menneskelige og tekniske ressurser og forutsetninger allerede på plass.

Realiseringen av strategien vil imidlertid kreve samordning og samhandling i en helt annen grad enn det som nå er tilfelle. Eksempelvis kan nevnes samordning mellom eksisterende sektortiltak og sektorovergripende tiltak, mellom defensive og offensive tiltak, mellom offentlige og private virksomheter, og samordning over landegrenser. Økt samordning og samhandling vil kreve endringer på flere plan. Disse knytter seg først og fremst til opparbeidelse av en felles situasjonsforståelse, tilpasning av regulatoriske rammefaktorer, teknisk tilrettelegging og utvikling av intern rolleforståelse og virksomhetskultur hos ulike aktører.

Det må påregnes administrative konsekvenser for berørte virksomheter ved oppfølging av tiltak som berører samordning og samhandling nasjonalt og internasjonalt. Hovedsakelig vil dette være i form av personalressurser. Nødvendig samordning og samhandling vil imidlertid også kreve ressursinnsats rettet mot blant annet tekniske løsninger for sikker kommunikasjon og krisehåndtering.

## Tiltak som antas å få vesentlige konsekvenser

Enkelte av de foreslåtte strategitiltakene vil ikke ha nevneverdige konsekvenser i seg selv, men vil kunne utløse aktiviteter hvor de økonomiske konsekvensene må vurderes nærmere på et senere tidspunkt. Eksempler på slike tiltak vil være FoU-program (tiltak nr. 2) og nedsettelse av lovutvalg (tiltak nr. 10).

Andre tiltak antas få vesentlige økonomiske eller administrative konsekvenser mer umiddelbart. Utvikling og implementering av sikre og robuste kommunikasjonsløsninger for

krisehåndtering (tiltak nr. 8) vil kreve investeringer og bør utredes nærmere. Dette vil blant annet forutsette en mer detaljert kartlegging av eksisterende løsninger.

Utvikling av felles krav til kritiske IKT-systemer (tiltak nr. 6) vil innebære kostnader som bør utredes nærmere.

Etablering av CSIRT-miljøer i de enkelte samfunnssektorer (tiltak nr.15) må bekostes av den enkelte sektor. Avhengig av ambisjonsnivået, vil det kunne påløpe både investeringskostnader og økte personellressurser. Det kan imidlertid også være snakk om omdisponering av eksisterende personell eller endrede arbeidsformer for å ta ut synergieffekter.

Forslag om etablering av et nasjonalt cybersenter (tiltak nr. 21) vil forutsette økninger både i investeringer, tilførsel av personalressurser og økte driftsmidler. Cybersenteret vil måtte utvikles over tid for å møte et IKT-risikobildet i stadig endring og den langsiktige videreutviklingen må utredes nærmere. Senteret anses å være et utgangspunkt og en suksessfaktor for gjennomføring av flere sentrale tiltak i strategien. Cybersenteret vil legge forholdene til rette for et nærmere samarbeid mellom EOS-tjenestene, politiet, sentrale sektormyndigheter, og private virksomheter. I tillegg er dette helt nødvendig for å få på plass en nødvendig beredskap og evne til å håndtere alvorlige angrep på IKT-systemer i Norge. Det understrekes at cybersenteret vil være en naturlig videreutvikling av NorCERT-funksjonen slik denne er etablert i dag.

## Gevinster som følge av styrket cybersikkerhet

Slik NSM ser det, er det i Norge i dag – i likhet med i mange andre sammenlignbare land – manglende samsvar mellom faren for alvorlige IKT-hendelser og konsekvensen av disse på den ene siden, og på den andre siden, effekten av eksisterende forebyggende sikkerhetstiltak og tilgjengelige operative kapasiteter for å håndtere og møte et IKT-risikobilde i endring. Dette gapet vil etter NSMs mening øke om det ikke settes inn effektive tiltak.

Strategien har som formål å ta igjen det eksisterende gapet og legge grunnlag for en kosteffektiv videreutvikling som sørger for robusthet rundt kritiske IKT-systemer med tilhørende operativ evne til å håndtere alvorlige situasjoner. Strategien vil slik sett bidra til å trygge befolkningens velferd, næringslivets videreutvikling, kritiske samfunnsfunksjoner og nasjonal sikkerhet. Strategien vil også bidra til at Norge kan fremme sine interesser internasjonalt og oppfylle sine forpliktelser vis a vis allierte.

En realisering av strategiforslaget antas å gi styrket samfunnsmessig evne til å stå i mot alvorlige angrep mot kritisk IKT-infrastruktur, og om angrep likevel skulle bli gjennomført gi styrket evne til å begrense skadeomfanget og evne til rask gjenoppretting av systemene.

En fokusert og bevisst satsning på cybersikkerhet vil også bidra til at Norge og norske miljøer fremstår koordinert, er kompetente og at vi dermed opprettholder vår posisjon som en

interessant samarbeidspartner internasjonalt. For et lite land som Norge vil dette være av stor betydning så vel for myndighetene som for akademia og relevante deler av næringslivet.

Om man søker å tilnærme seg IKT-risikobildet ved å prioritere sektorspesifikke løsninger vil man slik NSM ser det ikke få utnyttet de positive synergier og gjenbruk av løsninger som en tverrsektoriell tilnærming legger til rette for. Sektorspesifikke løsninger vil slik sett kunne være fordyrende økonomisk og samtidig kompliserende og forsinkende teknisk og operativt. I tillegg innebærer det nettverksbaserte samfunnet at eksisterende skiller mellom sektorene er i ferd med å viskes ut, da sektorenes IKT-systemer blir mer og mer gjensidig avhengig av hverandre. NSM vil derfor sterkt advare mot en utvikling der man i cybersikkerhetsarbeidet utelater behovet for sterkere samordning.

Med hilsen

Kjetil Nilsen
Direktør
Sjef Nasjonal sikkerhetsmyndighet