Norges vassdrags- og energidirektorat

NVE

Forsvarsdepartementet
Postboks 8126 Dep
0032 OSLO

Vår dato:
Vår ref.: NVE 201001660-9 aj/anro
Arkiv: 008
Deres dato:
Deres ref.: 2010/00794-1/FD I 5/OFD

Saksbehandler:
Anne Rogstad
22 95 91 46

Høringssvar - Forslag til strategi for cybersikkerhet

Innledning

Vi viser til brev av 30. mars 2010 med høring på forslag til strategi for cybersikkerhet med høringsfrist 25. juni 2010.

Vi viser også til at NVE ved seksjon EB i 2009 har gitt tilbakemelding på et tidligere utkast til strategi til en prosjektgruppe i NSM. NVE tok da forbehold om å komme med utdypende og utvidede uttalelser i forbindelse med den planlagte formelle høringsrunden.

Generell kommentar

NVE støtter i hovedsak målsettingen i forslaget, som reflekterer den gjensidige avhengigheten av kritiske IKT- systemer som eksisterer i et moderne samfunn, både nasjonalt og internasjonalt, og derigjennom behovet for et nasjonalt cybersenter som vil bidra til økt effektivitet i håndtering av omfattende nettbaserte IKT-hendelser.

NVE ønsker likevel å påpeke at det er en uklarhet i forhold til strategiens offensive innretning. NVE mener at foreliggende forslag ikke redegjør tilstrekkelig for hvorvidt den offensive innretningen av tiltakene er avgrenset i forhold til sivile og/eller militære formål. Det er heller ikke klart om den offensive innretningen er avgrenset til etterretningsvirksomhet med formål å oppdage og forhindre uønsket aktivitet, det være seg hos trusselaktører som er økonomisk, politisk eller militært motiverte. Dette er viktig i forhold til balanse mellom offensive og defensive tiltak, samt i forhold til mulige konsekvenser, styring og politiske akseptkriterier for offensive tiltak.

Spesielle kommentarer

Kommentarene nedenfor er gitt med referanse til det enkelte kapittel i utkastet til strategi. Der enkelte punkter eller tiltak ikke er nevnt i det nedenstående, betyr det at NVE ikke har spesielle kommentarer.

E-post: nve@nve.no, Internett: www.nve.no, Postbokс 5091, Majorstuen, 0301 OSLO, Telefon: 22 95 95 95, Telefaks: 22 95 90 00
Org.nr.: NO 970 205 039 MVA Bankkonto: 7694 05 08971

Hovedkontor
Drammensveien 211
0212 OSLO

Region Midt-Norge
Vestre Rosten 81
7075 TILLER
Telefon: 72 89 65 50

Region Nord
Kongens gate 14-18
Postboks 394
8505 NARVIK
Telefon: 76 92 33 50

Region Sør
Anton Jenssensgate 7
Postboks 2124
3103 TØNSBERG
Telefon: 33 37 23 00

Region Vest
Naustdalsvn. 1B
Postboks 53
6801 FØRDE
Telefon: 57 83 36 50

Region Øst
Vangsveien 73
Postboks 4223
2307 HAMAR
Telefon: 62 53 63 50

1.1. Hvorfor trenger vi en strategi?

Side 4 – 6.avsnitt
" .. *Sikkerhetstiltakene skal beskytte, ikke utfordre, grunnleggende rettigheter*.."

NVEs kommentar:
Her forstår NVE det som at det er tale om grunnleggende rettigheter for enkeltindivider og sivile virksomheter. Det bør kanskje presiseres i teksten. I forhold til påfølgende avsnitt (side 5) " *På den annen side*…" bør det tydeliggjøres at utfordringen det siktes til er en avveining mellom hensyn til konsekvensene for det enkelte individ / den enkelte virksomhet og for samfunnsmessige / nasjonale funksjoner/ interesser.

Side 5- Kort om strategien og enkelte kjernebegreper
"*Begrepet **cybersikkerhet** representerer* …."

NVEs kommentar:
Forklaringen av begrepet cybersikkerhet framstår som svært uklar og lite presis – hva ligger i formuleringen "*videreutvikling av informasjonssikkerhetsbegrepet*" og "*gjenspeiler samfunnets stadig økende avhengighet av IKT-systemer bundet sammen i cyberspace*."?

NVE mener at et så sentralt begrep - omfanget av strategien – bør ha en mer presis definisjon. NVE antar at begrepet cybersikkerhet i dokumentet kan relateres til informasjonssikkerhet som omfatter forebygging og håndtering av særlig alvorlige anslag, ondsinnede aktiviteter og nettbaserte angrep mot IKT-systemer som understøtter kritiske samfunnsfunksjoner. Dette framgår ikke av definisjonen. Det framgår heller ikke at fokus i strategien (ref. forklaring til "alvorlige IKT-hendelser" i avsnittet under) er å motvirke uønskede villede handlinger.

Strategien bør inneholde en forklaring på ord og uttrykk (se for eksempel Nasjonale retningslinjer for informasjonssikkerhet 2007-2010) og bruk av disse bør kvalitetssikres gjennomgående i dokumentet. I den grad dokumentet bruker begreper som er en videreutvikling av begrepet informasjonssikkerhet, bør dette relateres til en eksplisitt definisjon, for eksempel som den fra de nevnte nasjonale retningslinjer.

2.1 Etablere en felles situasjonsoversikt og forståelse

Side 14 under Tiltak 1:
Det står:
"*1. Kartlegge og verdivurdere kritiske IKT-systemer i alle sektorer*
I flere samfunnssektorer er det etablert prosesser for å kartlegge IKT-systemer av betydning for sektoren. Prosessene er imidlertid ikke samordnet. Gjennom sikkerhetslovens bestemmelser om informasjonssikkerhet og objektsikkerhet får man et sektorovergripende grunnlag for utvelgelse av systemer av vital nasjonal sikkerhetsinteresse.
…..
Basert på eksisterende prosessmekanismer og eksisterende kunnskap bør det nå iverksettes en samordnet prosess for løpende kartlegging og verdivurdering av kritiske IKT-systemer i alle sektorer. Samtlige sektormyndigheter med sikkerhetsansvar bør trekkes aktivt inn i arbeidet."

NVEs kommentar:
For kraftsektoren er en slik verdivurdering allerede gjort innenfor rammen av Energiloven.
I Forskrift for beredskap i kraftforsyningen (BfK - FOR-2002-12-16-1606), er det definert et system for kartlegging og verdivurdering av anlegg, inklusive kritiske IKT-systemer. NVE henviser for øvrig til høringsuttalelse som NVE gav til utkast til objektsikkerhetsforskrift i desember 2009. Der påpeker NVE også at ingen enheter i kraftforsyningen er underlagt sikkerhetsloven. Utpeking av

skjermingsverdige objekter i kraftforsyningen, herunder kritiske IKT-systemer, vil derfor ha en begrenset virkning dersom denne baseres på sikkerhetslovens bestemmelser om informasjonssikkerhet og objektsikkerhet.

Hvis kritiske IKT-systemer i kraftforsyningen skal fanges opp i en samordnet prosess, mener NVE at det er nødvendig at relevant lovverk for kraftforsyningen benyttes for kartlegging og verdivurdering av IKT-systemer i sektoren.

NVE viser herunder videre til vårt høringssvar til utkast til objektsikkerhetsforskrift:

- Etter NVEs oppfatning vil den generelle reguleringen av objektsikkerhet ha stor betydning for vitale objekter innenfor sektorer som ikke allerede har et velfungerende reguleringsregime for objektsikkerhet innenfor sin sektorlovgivning.

- Det er likevel NVEs oppfatning at objekter som følger energiloven og vannressursloven bør unntas fra objektsikkerhetsforskriften. NVE begrunner dette med at disse objektene allerede er underlagt detaljerte krav til objektsikkerhet i forskrift om beredskap i kraftforsyning (beredskapsforskriften) og den nye forskriften om sikkerhet ved vassdragsanlegg (damsikkerhetsforskriften). Bestemmelsene i disse forskriftene gjelder beredskap og sikkerhet mot skade som følge av krig, terror, sabotasje, teknisk svikt og naturgitte hendelser. NVE ønsker å unngå at de skjermingsverdige av disse objektene også skal omfattes av objektsikkerhetsforskriften slik at man får to tilnærmet parallelle regelsett som de ulike objekteierne må forholde seg til samtidig og som i tillegg forvaltes og følges opp av ulike tilsynsorganer. Dessuten vil det innebære en stor utfordring at den altoverveiende del av objektene innenfor kraftforsyningssektoren er eid av virksomheter som ikke er underlagt sikkerhetsloven.

Tilsvarende forhold kan gjelde andre sektorer også.

Arbeidet må bygge på de ulike sektorers sektorspesifikke lovverk og etablerte prosesser for innmelding av hendelser og myndighetsoppfølging.

2.1 Etablere en felles situasjonsoversikt og forståelse

Side 15 under Tiltak 2:
"*…For å skape en mest mulig helhetlig prioritering og langsiktighet i FOU-aktiviteter på cybersikkerhetsområdet bør JD og FD, med faglig støtte av etatene, gå sammen om å etablere et langsiktig FOU-program. Dette bør omfatte så vel sikkerhetsfaglige prosjekter som juridiske og policymessige. …*"

NVEs kommentar:
Et slikt tiltak er av interesse for NVE både i form av bidrag til aktuelle problemstillinger, sektorfaglig kompetanse og mulig del-finansiering. Et eksempel på problemstillinger er å finne effekten av bruk av sikkerhetssertifiserte komponenter i kritiske IKT-systemer, samt å kartlegge tilgang på slike (ref. tiltak 6).

Et FOU-program må sikres finansiering og en modell for forutsigbar finansiering må inngå som en viktig del av etableringen. Det er videre viktig at FOU-programmet får et innhold som er forankret i denne strategien.

Side 15 – Tiltak 3. Styrke kapasitet for vedlikehold og formidling av IKT-risikobildet

NVEs kommentar:
NVE forutsetter også at tiltaket bidrar til å forbedre formidlingen av oppdatert risiko- og eller trusselbilde til sektorene, både til sektormyndigheter og viktige virksomheter i den enkelte sektor.

Side 15 – Tiltak 5. Etablere partnerskap mellom offentlige myndigheter og private aktører
"*.. NorCERT der private virksomheter, offentlige myndigheter og etater samarbeider alt i dag for å oppdage og håndtere alvorlige IKT-hendelser er et eksempel på slikt partnerskap, og kan stå som modell for andre sider av cybersikkerhetsarbeidet ..*"

NVEs kommentar:
NVE anser NorCERT som et viktig tiltak for IKT-sikkerheten.
NVE mener at NorCERT må bli mer aktiv mot sektormyndigheter og være mer åpen enn tilfellet er i dag. Dagens modell der deler av NorCERTs aktiviteter (eksempelvis VDI) finansieres og reguleres av kommersielle avtaler, må ikke ligge til hinder for god og relevant informasjonsutveksling mellom NSM v/NorCERT og andre myndigheter. En grenseoppgang av informasjonsutveksling myndigheter og hvordan dette ivaretas i avtaler mellom offentlige myndigheter og private aktører imellom bør være en del av tiltaket.

2.2 Bygge og opprettholde robuste og sikre IKT-systemer

Side 16 – Status, kulepunkt 2.
" *Markedsmekanismer, samfunnsutviklingen og den teknologiske utvikling har medført at drifting av datasystemer har blitt lagt til land med kompetanse og lavt kostnadsnivå (såkalt offshoring). Dette skaper sårbarheter*."

NVEs kommentar:
Her bør det presiseres at drifting av datasystemer *i økende grad* har blitt lagt til land med kompetanse og lavt kostnadsnivå. Dette gjelder i varierende grad virksomheter i de ulike sektorer, i kraftsektoren ikke i det hele tatt eller i svært liten grad.

Side 16 – Tiltak 6. Stille felles krav til kritiske IKT-systemer
"*.. Det finnes teknologiske og administrative mottiltak som i sum kan utgjøre et godt forsvar i dybden mot mange typer angrep. Krav og tiltak som forutsettes til stede i kritiske IKT-systemer, inkludert hvordan disse bør designes, konfigureres, driftes og vedlikeholdes med tanke på best mulig sikkerhet er ikke godt nok utviklet. Tiltakene bør derfor videreutvikles og nedfelles i krav som er felles for kritiske IKTsystemer. Dette inkluderer også å se på krav til fysisk beskyttelse, retningslinjer for offshoring m.m.…*"

NVEs kommentar:
Felles krav til informasjonssikkerhet i kritiske IKT-systemer må utvikles i nært samarbeid med de enkelte sektormyndigheter for å ivareta særlige behov. Det kan for eksempel være ulike hensyn som skiller for eksempel styrings- og kontrollsystemer fra transaksjonssystemer mhp. krav til tilgjengelighet, integritet og konfidensialitet. Dette kan også være forhold som begrenser hvilke felles krav som kan stilles.

Side 16 – Tiltak 7. Styrke tilsyn med IKT-sikkerhet
"*.. Tilsyn med IKT-sikkerhet gjennomføres i dag av flere myndighetsorganer som i liten grad utveksler tilsynserfaringer. Det samlede tilsynsarbeidet med sikkerheten i IKT-systemene, så vel tverrsektorielt som sektorvis, bør kartlegges og gjennomgås med tanke på forbedringer og samordning. Erfaringene bør samles og analyseres, og gi føringer for videreutvikling av sikkerhetstiltak og koordinert gjennomføring av tilsyn...*"

NVEs kommentar:
NVE utfører i dag tilsyn med beredskap i kraftsektoren og har etablert samarbeid med DSB som har tilsyn med sikkerhet i elektriske anlegg. Det er etablert et tilsynsforum for dette samarbeidet og det er gjennomført felles tilsyn for å få erfaring med dette. NVE har også invitert NSM/NorCERT til samarbeid knyttet til tilsyn med beredskap, herunder informasjonssikkerhet for kritiske IKT-systemer i kraftsektoren. NVE har videre løpende kontakt med Post- og teletilsynet og Norsk senter for

informasjonssikring.

Ut fra NVEs erfaring med tilsyn og samarbeid i tilknytning til dette, mener NVE at koordinering av tilsyn er mest effektivt gjennom utveksling av faglig erfaring i et tilsynsforum, ikke gjennom felles tilsyn. NVE anbefaler derfor at etablering av et tverrsektorielt tilsynsforum for IKT-sikkerhet bør inngå som en del av dette tiltaket.

Side 17 – Tiltak 8. Utvikle og implementere sikre og robuste kommunikasjonsløsninger for krisehåndtering

NVEs kommentar:
Kraftforsyningen har i dag et kommunikasjonssystem for tale som benyttes for krise-håndtering i kraftforsyningen mellom myndigheter og private virksomheter. Dette er imidlertid ikke kvalifisert for å utveksle informasjon gradert etter Sikkerhetsloven. NVE ønsker å videreutvikle dette kommunikasjonssystemet til også å omfatte meldingsbasert utveksling av kraftsensitiv informasjon (taushetsbelagt etter Forskrift for beredskap i kraftforsyningen). Det er ønskelig å samordne dette med et tilsvarende kommunikasjons-system for gradert informasjon.

NVE vil også bemerke at dagens system med kryptotelefon er basert på bruk av tjenester i de offentlige mobiltelefonnettene. Dette systemet er derfor omfattet av de samme sårbarheter som disse med henblikk på tilgjengelighet.

NVE vurderer også pr dags dato at Nødnettet ikke tilfredsstiller kraftforsyningens krav til tilgjengelighet, spesielt ved bortfall av ordinær kraftforsyning. Felles kommunikasjonsløsninger for krisehåndtering må derfor baseres på mer robuste kommunikasjonsnett enn tilfellet er i de eksisterende felles kommunikasjonsløsninger.

Side 17 – Tiltak 9. Videreutvikle beredskapsplaner med tanke på cybersikkerhetstiltak

NVEs kommentar:
Nasjonale beredskapsplaner bør utvikles i tett samarbeid med de ulike sektormyndighetene basert på sektorvise beredskapsplanverk, også for tiltak knyttet til informasjonssikkerhet i kritiske IKTsystemer.

Side 17 – Tiltak 10 Behov for regulatorisk forankring av cybersikkerhet

NVEs kommentar:
Det er tydelige krav til IKT-sikkerhet for kraftforsyningen gjennom Forskrift om beredskap i kraftforsyningen.

2.3 Bevisstgjøre, opplyse og påvirke

Side 18 – Tiltak 11. Styrke tiltak for bevisstgjøring, utdanning og holdningsskapende arbeid

NVEs kommentar:
NVE har tiltak for dette i form av å arrangere egne seminarer for kritiske IKT-systemer i kraftsektoren der informasjonssikkerhet er spesielle tema. I tillegg er NVE aktive innenfor holdningsskapende tiltak for informasjonssikkerhet både mot fagpersonell og ledelse i virksomheter med kritiske IKT-systemer. NVE ser stor nytte i et samarbeid knyttet til dette.

NVE etterlyser også at tiltaket adresserer behovet for at relevante deler av utdanningssektoren (høyskoler og universiteter) styrker tilbud og kapasitet for relevant kompetansegivende utdanning knyttet til informasjonssikkerhet. Dette er også viktig i forhold til dokumentert sikkerhetskompetanse.

2.4 Styrke evnen til å oppdage, varsle og håndtere IKT-hendelser

Side 19 – Tiltak 13 Styrke samfunnets evne til å oppdage trusler og sårbarheter

NVEs kommentar:
NVE støtter at VDI bør kunne utvides og videreutvikles. Det forutsettes da samtidig at systemet for å formidle oppdagelse av trusler og hendelser og formidle råd til sektormyndighetene videreutvikles og forbedres. Hendelser og informasjon av betydning for kraftforsyningen forutsettes raskt kommunisert til NVE som sektormyndighet (jf også tiltak 14 i strategiforslaget).

Se også NVEs kommentar til tiltak 5 ovenfor.

Side 19 – Tiltak 15. Etablere sektorvise CSIRT-miljøer i samfunnsviktige sektorer og i de største enkeltvirksomheter

NVEs kommentar:
NVE er positive til tiltak som styrker rask og systematisk varsling mellom sektorene ved alvorlige hendelser.

Ulike fora og nettverk er etablert innen kraftforsyningen. NVE stiller krav og understreker betydningen av å innrapportere hendelser innen kraftforsyningen og arbeider for å videreutvikle forsterkede mekanismer for informasjonsdeling og samvirke om IKT-sikkerhet i sektoren. Vi ønsker fortsatt god dialog og samråd med NSM i dette arbeidet.

2.5 Etterforske og bekjempe IKT-hendelser

Side 20 – Tiltak 17. Sikre mulighet til nødvendig lagring av data ved hendelser med tanke på å muliggjøre effektiv etterforskning

NVEs kommentar:
Tiltaket har vidtgående omfang, ref. også pågående prosess knyttet til Datalagringsdirektivet. Uten å ta stilling til innholdet av direktivet og omfanget av dette i særdeleshet, ønsker NVE at etater med ansvar for etterforskning og håndtering av målrettede dataangrep / datakriminalitet kan bistå sektormyndigheter med tilråding om og krav til hvilke data som bør innhentes og lagres for slike formål i kritiske IKT-systemer, inkludert anbefalinger om formålstjenlig lagringstid mv. Dette vil gi et godt grunnlag for at informasjon om tilrettelegging av datalagring for slike formål formidles til enkeltvirksomheter også i sektorspesifikk veiledning.

Relevante aspekter knyttet til personvern for ansatte i virksomhetene i tilknytning til slik lagring bør vurderes med hensyn på sikker lagring og restriksjoner for bruk av data lagret for disse formål.

Side 21 – Tiltak 20. Offensive kapasiteter

NVEs kommentar:
Når det gjelder offensive kapasiteter vil NVE understreke nødvendigheten av at slike tiltak om mulig bør koordineres med eventuelle berørte virksomheter slik at slike operasjoner ikke blir oppfattet som hendelser virksomhetene skal korrigere eller forhindre.

NVE vil også peke på at offensive tiltak fra norske myndighetsorganer (både sivilt og miltært) også vil kunne øke risikoen for eskalering av en eventuell konflikt som i seg selv utgjør økt trusselnivå for sivile virksomheter. Også i den forbindelse vil NVE peke på nødvendigheten av koordinering slik at for eksempel beredskapsnivået i det sivile samfunn kan økes tilsvarende.

2.6 Styrke samordning av cybersikkerhetssamarbeidet

side 21 - 2. avsnitt, siste setning
"*Det vil derfor være viktig å få gode krisehåndteringsmekanismer på plass som sørger for at hensyn avveies og at dette skjer på det rette ansvarlige nivå*."

NVEs kommentar:
Det bør presiseres at det er viktig at *både avveining av hensyn og beslutning* skjer på det rette ansvarlige nivå, ikke bare avveining av hensyn.

NVE anbefaler videre å se på hvordan man kan videreutvikle et mer formalisert samvirke mellom myndighetene på dette området. I dette samvirket forutsettes aktuelle sektormyndigheter å bli inkludert.

Vedlegg A Eksisterende roller, ansvar og myndighet nasjonalt

I tillegg til ulike offentlige organer, bør kanskje nevnes at det finnes ulike organisasjoner etablert som private/sivile initiativ, eksempelvis ITAKT, NSR og andre sektorvise organisasjoner. Både kraftsektoren og petroleumssektoren har fora for informasjonssikkerhet. Disse er relevante i forhold til tiltak for bevisstgjøring, holdningsskaping, kompetanseheving og partnerskap.

Oversendes uten underskrift. Kvalitetssikret i henhold til interne rutiner.

Med hilsen

Gunn Oland
avdelingsdirektør

Ingunn Åsgard Bendiksen
seksjonssjef