

Forsvarsdepartementet

Postboks 8126 Dep  
0032 Oslo

FORSVARSDEPARTEMENTET	
SAKNR.: 10 / 00794 - 18	
28 JUN 2010	
ARKBET:	206
KASSERES 5 ÅR	
KASSERES 30 ÅR	
BEVARES	

Vår ref.:  
2010/196 - 2968/2010

Deres ref.:  
201001542-/KRF

Saksbehandler:  
Johnny Heggestad, 51 96 38 31

Dato:  
25.06.2010

## Oversendelse av Forsvarsdepartementets høring om forslag til strategi for cybersikkerhet

Vi takker for invitasjon til høring og oversender herved våre kommentarer som angitt nedfor:

Helsesektoren har store mengder sensitive personopplysninger. Helse-Vest har prioritert fokus på informasjonssikkerhet og støtter derfor opp om de 22 tiltakene i høringsutkastet. Under er en kort gjennomgang av tiltakene med konsekvenser og merknader.

### ETABLERE EN FELLES SITUASJONSOVERSIKT OG FORSTÅELSE

#### **Tiltak nr 1 – Kartlegge og verdivurdere kritiske IKT-systemer i alle sektorer**

Et sektorielt perspektiv kan oppnås dersom arbeidet forankres og styres fra et overordnet nivå. Kunnskap om verdivurdering av kritiske IKT-systemer er begrenset, dette innebærer at ressurser må omprioriteres eller tilføres. En omprioritering kan få konsekvenser både for den daglige driften og prosjekter som er planlagt eller påbegynt.

#### **Tiltak nr 2 – Måltrettet satsing på forskning og utvikling**

Små eller ingen administrative eller økonomiske konsekvenser for Helse-Vest.

#### **Tiltak nr 3 – Styrke kapasitet for vedlikehold og formidling av IKT-risikobilde**

Ulike rapporteringskanaler bør etableres og koordineres slik at informasjonen når fram til dem som trenger den raskest mulig, uavhengig av rapporteringsmedium (for eksempel e-post, telefon, Internett). Et sektorielt perspektiv kan bare oppnås dersom dette arbeidet koordineres på et overordnet nivå.

#### **Tiltak nr 4 – Styrke det internasjonale samarbeidet om cybersikkerhet**

Utvexling av helseopplysninger over landegrensene kan være aktuelt både med hensyn til effektiv pasientbehandling og forskning. Dette forutsetter en sikkerhetsarkitektur som er basert på internasjonale standarder og avtaler regulert av overnasjonale og mellomstatlige organ, som eks NATO og EU.

### BYGGE OG OPPRETHOLDE ROBUSTE OG SIKRE IKT-SYSTEMER

#### **Tiltak nr 6 – Stille felles krav til kritiske IKT-systemer**

Krav om sertifisering på kritiske IKT-systemer kan medføre betydelige merkostnader for eksisterende IKT-systemer, samtidig vil innføringstiden for nye systemer øke.

#### **Tiltak nr 8 – Utvikle og implementere sikre og robuste kommunikasjonsløsninger for krisehåndtering.**

Administrative og økonomiske konsekvenser for Helse-Vest bør utredes. Behovet for å sikre kritisk infrastruktur mot skadelig elektromagnetisk puls(EMP) bør også vurderes.

## **BEVISSTGJØRE, OPPLYS OG PÅVIRKE**

### **Tiltak nr 12 – Arrangere og delta i øvelser**

De administrative og økonomiske kostnadene vil være avhengig av omfanget og hyppigheten av øvelser.

## **STYRKE EVNEN TIL Å OPPDAGE, VARSLE OG HÅNDBERE IKT-HENDELSER**

### **Tiltak nr 13 – Styrke samfunnets evne til å oppdage trusler og sårbarheter**

Økonomiske og administrative konsekvenser bør utredes.

### **Tiltak nr 14 – Legge til rette for innrapportering av hendelser**

Bedre tilrettelegging av rapporteringsrutiner kan medføre økt rapporteringsfrekvens som igjen kan få økonomiske og administrative konsekvenser. Samtidig er det rimelig å anta at ressursbehovet vil avta over tid. Spisskompetanse til å håndtere innrapporterte hendelser i et dynamisk trusselbilde er påkrevd. Tiltak 14 bør sees i sammenheng med læringseffekten av det å etablere sektorielle CSIRTer (tiltak 15).

### **Tiltak nr 15 – Etablere sektorvise CSIRT-miljøer i samfunnsviktige sektorer og i de største enkeltvirksomheter**

Forslaget legger opp til en selvfinansiert modell. Forankring, finansiering og avgrensning er kritiske suksessfaktorer for at arbeidet med å etablere sektorielle CSIRTer skal lykkes. Organiseringsform, finansieringsmodell og ambisjonsnivå bør derfor utredes.

*Kommentar: På oppdrag fra Sosial- og helsedirektoratet(SHDIR) har Norsk helsenett(NHN) tatt initiativ til å etablere en HelseCSIRT for helsesektoren. Helse-Vest har deltatt i dette arbeidet.*

## **ETTERFORSKE OG BEKJEMPE IKT-HENDELSER**

### **Tiltak nr 19 – Avdekke og identifisere trusler og trusselaktører**

Dette åpner for deltakelse i internasjonalt samarbeid.

## **STYRKE SAMORDNING AV CYBERSIKKERHETSARBEIDET**

Ingen kommentar

Med helsing  
Helse Vest RHF



Ivar Eriksen  
Eigardirektør



Johnny Heggstad  
Prosjektleder

Kopi: Helse- og omsorgsdepartementet