DnB NOR

Forsvarsdepartementet
Postboks 1826 Dep.
0032 Oslo

Attn. Gisle Norheim

Vår ref.	Deres ref.	Dato
DnB NOR IT/SN	2010/00794-1/FD I 5/OFD	OSLO, 25. juni 2010

Kommentarer til "Høring - forslag til strategi for cybersikkerhet"

DnB NOR takker for muligheten til å uttale seg på et sentralt tema som cybersikkerhet. Utkastet til nasjonal strategi for cybersikkerhet belyser mange av de samme temaene som DnB NOR fokuserer på for sine kunder. Det oppleves i dag at samfunnet har stor tillit til Internett og de samfunnsviktige funksjonene som bruker Internett som bærer. Derfor blir videre styrking av Norges kapasitet innen cybersikkerhet helt avgjørende for det videre tillitsnivået også for DnB NORs kunder. DnB NOR støtter retningen om samordning rundt sektorovergripende cybersikkerhetstiltak som vil gi økt situasjonsforståelse både innenfor de respektive sektoren og for samfunnet generelt.

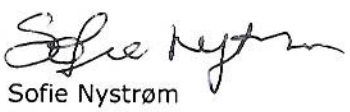
I tiltak 3 "vedlikehold og formidling av IKT-risikobilde" støtter DnB NOR retningen som er beskrevet, men savner tydelighet rundt hvordan man skal iverksette dette tiltaket. Det er av stor verdi for bankene å forstå sitt risikobilde i forhold til andre virksomheter både innenfor og utenfor sektoren. I internasjonalt samarbeid gjennom Information Security Forum (ISF) gjøres det jevnlig standardisert benchmarking mellom medlemmene. Denne dataen kan da virksomheten selv bruke i forhold til videre satsning og investering innenfor sikkerhet. Toppledelsen i de fleste virksomheter ønsker å vite hvor deres organisasjon er i forhold til andre sammenlignbare aktører.

Ved å styrke kapasiteten til å samle inn faktagrunnlag, sammenstille og formidle et IKT-risikobilde også sektorvis er derfor et veldig nyttig virkemiddel. Innskjerping av rapporteringsrutiner vil etter vår mening ikke alene være et effektivt virkemiddel for å nå målsettingen. Både POLF og IKT-forskriften pålegger vår næring å rapportere blant annet alvorlige sikkerhetsbrudd og -sårbarheter. Denne rapporteringen er nå innarbeidet i rutiner og det oppleves at dette er den mest hensiktsmessige varslingsveien. Gjenbruk av eksisterende rapportering som beskrevet i tiltak 14 støttes.

Etablering av sektorvise CSIRT-miljøer har vært diskutert over tid. Det er DnB NORs erfaring at det er meget varierende grad av hendelseshåndteringskompetanse innen dette området utenfor NorCERT og den enkelte virksomhet (inklusivt leverandører). Dette tiltaket krever derfor et stort fokus på utdannelse av spisskompetente hendelseshåndterere som kan bidra inne i de sektorvise CSIRT-mijøene. Det etterlyses også erfaringsgrunnlag fra andre land der slike sektorvise CSIRT er etablert og har gitt god nytteverdi i hendelser. Det er viktig at det blir god praktisk tilrettelegging slik at man får en effektiv hendelseshåndtering.

DnB NOR støtter videre etablering av et nasjonalt cybersikkerhetssenter hvor eksisterende initiativ som NorCERT og VDI blir grunnstenene til senteret.

Med vennlig hilsen
for DnB NOR Bank ASA



Sofie Nystrøm
Divisjonsdirektør, IT
Chief Information Security Officer