Norsk senter for informasjonssikring

Norsk senter for informasjonssikring

Postadresse:
Pb 104
N-2801 Gjøvik

Besøksadresse:
Merkantilvn 2
E-mail: post@norsis.no
URL: www.norsis.no

Tlf. +47 40 00 58 99

Det kongelige justis- og politidepartement
Postboks 8005 Dep
0030 OSLO

Kopi:
De kongelige fornyings- og administrasjonsdepartement

Deres ref.:	Vår ref.:	Direkte innvalg:	Gjøvik dato
200604470-RBA-K/LB/BHH	010.4/18/06	+ 47 93021853	23.10.2006

Høringsuttalelse fra NorSIS på «NOU 2006:6 Når sikkerheten er viktigst»

NorSIS har gjennomgått NOU 2006:6 Når sikkerheten er viktigst, og er generelt meget positiv til at sikkerhetsarbeidet settes på dagsorden fra myndighetenes side, og at konkrete forslag til bedring av sikkerheten i Norge legges frem. NorSIS har kommentarer og forslag knyttet til enkelte kapitler og punkter til NOU 2006:6.

Kapittel 3

- Rapporten beskriver at «et tett koplet system bare kan kontrolleres effektivt gjennom sentralisert styring». NorSIS mener at dette til en viss grad også kan gjelde innen tilsyn og kontroll av informasjonssikkerhet. Det er flere tilsyn og direktorater som kontrollerer, og dette synes å i mindre grad være sentralisert og koordinert. NorSIS mener det bør bestrebes etter en noe mer koordinert og helhetlig innsats i forhold til tilsyn, styring og bevisstgjøring av informasjonssikkerhet på overordnet nivå i Norge i dag.
- NorSIS mener det må klargjøres hva som kommer inn under «rikets sikkerhet». Det kan være systemer og virksomheter som vanligvis ikke er definert i begrepet, men som i en spesiell situasjon kan være omfattet av det. (kap 3.2)
- Vi mener det er meget viktig å fremme kunnskap om risikotankesettet for alle virksomheter i Norge – *ikke* bare de som er knyttet til landets kritiske samfunnsfunksjoner (kap 3.3)
- Vi er enige i forvirringen knyttet til ordbruk. NorSIS ser det som en fordel at definisjoner og begreper knyttes til sikkerhet forenkles i størst mulig grad. Personer som arbeider med sikkerhet vil ha lett for å lære seg ulike ord og uttrykk, men for de aller fleste i Norge mener NorSIS det vil være viktig å benytte et så ordinært og enkelt språk som mulig. NorSIS foreslår som NOU-en beskriver at «sikkerhet»

dekker alle aspekter. Trygghet og sikring vil i det daglige bli brukt om hverandre, selv om fagmiljøene forsøker å skille de ad. I stede for tilsiktede og utilsiktede hendelser foreslår NorSIS at det benyttes bevisste (tilsiktede) handlinger og ubevisst (utilsiktede). (kap 3.10)

Kapittel 4

- Små og mellomstore virksomheters dataressurser, som ikke er tilstrekkelig sikret kan bli roboter i et botnet. De kan dermed bidra til at større angrep kan bli gjennomført. Det må derfor bli et samfunnsansvar at alle sikrer sine maskiner, for å unngå å bli et verktøy for bevisste angripere. (kap 4.2.6.1)

Kapittel 5

- Mørketallsundersøkelsen fra Næringslivets Sikkerhetsråd (NSR) viser at det er usikkerhet om virksomheten er en del av kritisk infrastruktur eller ikke. NorSIS mener det er viktig å avklare dette nærmere, og at det bør brukes en bred definisjon av det. Med dagens teknologi er mye knyttet sammen og er avhengige av hverandre. Mange utkontrakterer tjenester og det er ikke like lett å avgrense hva som er nødvendig for å drifte den kritiske infrastrukturen og samfunnsfunksjonene. (kap 5.4.3)
- NorSIS mener at det utad er noe vanskelig å se at Norge har ett «sikkerhetsdepartement» (kap 5.4.1).
- NorSIS mener det er veldig viktig å få en felles metode og system for å peke ut hva som er kritisk infrastruktur og kritisk samfunnsfunksjoner (kap 5.4.1)
- NorSIS er veldig fornøyd med at alle virksomheter med ansvar for kritisk infrastruktur og kritisk samfunnsfunksjoner får et felles sett prinsipper for sikkerhet. Disse prinsippene bør i størst mulig grad også selges inn til **alle** andre virksomheter i Norge. NorSIS ser dette som en av sine viktige oppgaver, og vil bidra til størst mulig spredning av disse prinsippene. NorSIS har noen forslag til endringer til prinsippene:

  1. Sikkerhet må forankres og ha høy status hos ledelsen.
  2. Sikkerhet og beredskap skal være en integrert del av virksomhetens drift og må omfatte sikkerhetsledelse, fysisk sikkerhet, personellsikkerhet, informasjonssikkerhet og IT-sikkerhet.
  3. Virksomheten skal til enhver tid ha en oppdatert oversikt over roller og ansvar for sikkerhet og beredskap. *(Dette punktet i NOU-en kan synes for detaljert i forhold til de andre prinsippene)*
  4. Sikkerhetstiltakene skal til enhver tid stå i forhold til sikkerhetsrisikoen, som identifiseres gjennom risikoanalyser.
  5. Virksomheten skal sette seg mål og standarder for sikkerhetsarbeidet. Gjennom godt lederskap og god virksomhetsstyring skal det følges opp at målene nås og standardene følges.
  6. God sikkerhet skal bygges på riktige holdninger blant medarbeiderne. Virksomheten må ha et system for opplæring innen etikk, sikkerhet og beredskap for å understøtte dette.

7. Alle medarbeidere har ansvar for å følge prinsipper og standarder for sikkerhet.
8. Virksomheten bør ha system for deling og kontroll av informasjon, både internt og eksternt. *(Dette punktet i NOU-en kan synes for detaljert i forhold til de andre prinsippene)*
9. Når uønskede hendelser inntreffer, skal beredskapstiltak bidra til å begrense skaden og bringe virksomheten tilbake til normal drift.

- NorSIS støtter at det utarbeides en informasjonshåndbok hvor det fremgår hva de ulike myndighetsorganene kan tilby av råd og veiledninger. Informasjonshåndboken må være elektronisk og det må besluttes hvem som er ansvarlig for å holde den oppdatert. NorSIS anser seg som en relevant instans til å ta en slik oppgave (kap 5.4.4).

Kapittel 6

- Lovreguleringen kan synes komplisert i dag, men NorSIS mener de lovene som eksisterer i dag er nødvendig og gir myndighetsapparatet et verktøy for å håndheve og kontrollere informasjonssikkerheten i Norge (kap 6.1).
- NorSIS støtter arbeidet med en ny lov knyttet til beredskap. Vi mener loven kan være knyttet til sikkerhet, som vi mener er et mer omfattende begrep, da beredskap gjerne ses på som en del av sikkerhetsarbeidet - i de tilfeller sikringstiltakene ikke er tilstrekkelige og alvorlige hendelser skjer. Temaene som tenkes berørt i loven omfatter mer enn beredskapsaspektet (kap 6.6.1).
- Det finnes mange generelle lover for å regulere sikkerhet i samfunnet, hvor det stilles krav til f eks alle innbyggere (f eks trafikksikkerhet) eller alle virksomheter (f eks HMS arbeid). NorSIS mener det bør vurderes om den nye lovens virkeområde kan omfatte alle virksomheter. (kap 6.6.1)
- Det er vesentlig at loven klart beskriver hva som kreves av den enkelte virksomhet, slik at overholdelse av loven og tilsyn av overholdelse blir mulig.
- Vedr offentlige innkjøp bør det også stilles krav til sikkerhet i selve leveransen (ikke bare ved bortfall av varer og tjenester) (Kap 6.6.4)

Kapittel 10

- Etter hvert som bruken og avhengigheten til IKT øker i samfunnet vil det være et behov for bedre informasjonssikkerhetsmekanismer og mer bevissthet hos brukerne. Dette på samme måte som økt bruk av biler krever bedre infrastruktur og holdninger til at alle brukerne f eks bruker bilbelte. (kap 10.1.3). Det offentlige må her ta et spesielt ansvar (jfr kap 8.1.1 og tabell 10.1), da markedet ikke ennå ser ut til å fungere mht sikkerhetsprodukter knyttet til informasjonssikkerhet og at brukere må bevisstgjøres til å ha en god sikkerhetskultur.
- NorSIS er enig med utvalget i at for å oppnå en bedre informasjonssikkerhet må det diskuteres om den enkelte tilbyder og leverandør skal pålegges å levere sikkerhetsløsninger som gjør det enkelt for brukeren å oppnå en tilfredsstillende sikkerhet (kap 10.1.4).
- NorSIS støtter riksrevisjonens og utvalgets anbefalinger knyttet til organisering av sikkerhetsarbeidet om avklaring av ansvarsforhold for sikkerhet. Det er imidlertid

litt uklart hva NOU-en beskriver knyttet til sammenslåing av FADs og SDs sammenslåing og ansvar for informasjonssikkerhet.

Merknader rettet mot vårt virkeområde

- NorSIS nevnes ikke som et av de pedagogiske virkemidlene i kap 6.4. NorSIS er et permanent senter og en del av den helhetlige offentlige satsningen innen informasjonssikkerhet i Norge. NorSIS har små og mellomstore virksomheter i privat sektor, og offentlig sektor, herunder kommunene som målgruppe. Vi arbeider forebyggende og bevisstgjør om trusler og sårbarheter, opplyser om tiltak og påvirker til gode holdninger og god sikkerhetskultur. Vi har et nært samarbeid med Post og teletilsynet (www.nettvett.no), som har forbrukerne som sin viktigste målgruppe, Medietilsynet (www.saftonline.no), som har barn og ungdom som sin viktigste målgruppe og Nasjonal sikkerhetsmyndighet ved VDI/ NorCERT, som har den kritiske infrastruktur som sin viktigste målgruppe. Forskjellige målgrupper krever forskjellige virkemidler.
- NorSIS har fått andre oppgaver fra 1.1.2006, og skal ikke lenger samle inn informasjon om hendelser, men NorSIS lager månedlige rapporter om ulike aspekter ved sikkerhet slik at SMB og off sektor kan få et overblikk over hva som skjer. (kap 6.6.6)
- NorSIS ser at omorganisering av sikkerhetsarbeidet, slik at ett departement har ansvaret for IT-sikkerhet, medfører en endring for oss. NorSIS ser behovet for en samordnet og koordinert satsning på dette viktige fagfeltet som en styrke (kap 10.1.4 og kap 13.2).

Forslag til andre virkemidler

- NorSIS mener det er nødvendig med et større løft, f eks en kampanje fra staten rettet mot befolkningen og blant små og mellomstore virksomheter for å bevisstgjøre om trusler og sårbarheter og opplyse om viktige sikringstiltak. NorSIS jobber aktivt med å planlegge en større kampanje for å øke bevisstheten til informasjonssikkerhet mot vår målgruppe. En utfordring er at slike kampanjer (TV, radio, media) er ressurskrevende. NorSIS ser allikevel at det er et stort behov for en folkeopplysning på dette området.
- NOU-en beskriver i meget liten grad beskyttelsesinstruksen og dens krav, men tillegger sikkerhetsloven et helt kapittel. NorSIS stiller spørsmål ved hvorfor beskyttelsesinstruksen ikke er beskrevet i NOU-en.

Med vennlig hilsen

Tone Hoddø Bakås
seniorrådgiver
NorSIS