UNIVERSITETET
I OSLO

Forsvarsdepartementet
Postboks 8126 Dep
0032 OSLO

Universitetets senter
for
informasjonteknologi
Postboks 1059

0316 Oslo

Informatikkbygningen
Gaustadalléen 23
Telefon: 22 85 24 70
Telefaks:22 85 27 30

Blindern

Dato: 02.07.2010
Deres ref.: 2010/00794-1/FD I 5/OFD
Vår ref.: 2010/4728

Høringssvar til strategi for cybersikkerhet

Universitetet i Oslo (UiO) ved Universitetets senter for Informasjonsteknologi (USIT) er landets største drifts- og utviklingsmiljø innenfor universitets- og høyskolesektoren.

UiO ved USIT arbeider mye med IT-sikkerhet i virksomhetens drifts- og utviklingsmiljøer og gjennom egen IT-sikkerhetsorganisasjon og CERT-gruppe.

UiO mener NSD og NorCERT bør ha en sentral rolle i arbeidet med å sikre de informasjonsverdiene vi alle stadig blir mer avhengige av og at det gjennom høringen er satt viktige problemstillinger på dagsorden.

I all hovedsak er universitetet enig i de vurderingene som legges til grunn og forslagene til iverksetting som legges fram i "Nasjonal strategi for Cybersikkerhet". Universitetet vil derfor i denne høringsuttalelsen kun noen av de konkrete tiltakene som foreslås:

Punkt 2.1, tiltak 2-3
Universitetet er enig i at det trengs mer forskning og utvikling på områdene. Det bør også utarbeides risikobilder fra flere parter slik at risikobildet ikke kun gjenspeiler hva enkelte internasjonale aktører fremlegger, men det faktiske trusselbildet i ulike sektorer i Norge.

Punkt 2.1, tiltak 4
Flere gode spydspisstiltak er allerede iverksatt i Europa på dette området, bla sentralt i EU og i Sveis.

Punkt 2.1, tiltak 5
Det fremstår for UiO som viktig å også få andre aktører enn NorCERT/NSM til å vurdere verdien av det gjeldende IT-sikkerhetssamarbeidet.

Punkt 2.2 tiltak 6
Sikkerhetsrisiki ved å pålegge bedrifter å følge NSMs sertifiseringsstrategi bør kartlegges. Systemer etter denne modellen er dyre, tunge i vedlikehold og i seg selv komplekse å sikkerhetsoppdatere.

Det legges så vidt vi forstår opp til en situasjon hvor NSM skal foreta tunge, langvarige og grundige sertifiseringer av elementer i relativt lave lag, f.eks. infrastruktur, OS mv.

UiO oppfatter ikke dette som et godt virkemiddel for de sikkerhetsutfordringene som eksisterer i dag. I tillegg vil tunge sertifiseringer av denne typen kunne ekskludere endel OpenSource løsninger og/eller produkter fra mindre firma fra markedet. En slik løsning vil potensielt kunne skape problemer for produkter og tjenester som UiO er avhengige av. Dette vil etter vår oppfatning være svært uheldig.

Samtidig ser vi at de reelle sårbarhetene vi møter i hverdagen forblir uadresserte fra såvel leverandører som myndighetene. Om det avdekkes alvorlige sårbarheter i for eksempel et elektronisk saksbehandlingssystem som er utbredt i det offentlige, finnes det i dag ingen sentral myndighet som kan håndtere en slik hendelse, verken i forhold til de virksomhetene som anvender løsningen eller i forhold til leverandøren. UiO mener en slik viktig rolle naturlig bør ligge hos NSM.

Punkt 2.4
UiO mener det ville vært hensiktsmessig om NorCERT økte sin kapasitet til å samarbeide med private virksomheter som er under angrep.

I statuspunkt 2 nevnes "få virksomheter har nødvendige rutiner og deteksjonsmekanismer", i samme setning som VDI. UiO mener at NorCERT/NSM burde ha nødvendig kapasitet til å veilede virksomheter som deltar i VDI-samarbeide på dette området.

Punkt 2.4 tiltak 13
Norge er i dag midt i en debatt om datalagring og for hvilke formål ulike typer overvåking og datalagring lar seg forsvare. Strategien kommer med ulike tiltaksforslag som uten nødvendig presishet såvel foreslår å øke omfanget av varslingssystemer (VDI, tiltak 13) som å "sikre muligheten til nødvendig lagring av data..." i tiltak 17.

UiO mener det er viktig å ha et høyere presisjonsnivå denne typen forslag og formuleringer som omhandler overvåking, datalagring og sammenkobling av data, slik at det for alle involverte er klart hva de innebærer.

Punkt 2.4 tiltak 15
Funksjonene "CSIRT for kritisk infrastruktur" og "nasjonal CSIRT" bør adskilles. Den nasjonale CSIRT-funksjonen bør være koordinerende funksjon for alt fra den nevnte kritisk intrastruktur-CSIRT til ISP-enes CSIRT og Akademia. NorCERT har i dag rollen som CSIRT for kritisk infrastruktur. En rolleblanding her kan være uheldig.

Punkt 2.5 Statuspunkt 3
Etter UiO sin oppfatning fremstår dette primært som et kapasitetsproblem hos KRIPOS og vil ikke avhjelpes med flere aktører på banen.

Punkt 2.5 tiltak 17
Hensynet til enkeltindividers rettssikkerhet tilsier etter UiOs mening at man bør være svært varsom med å endre dagens ordning.

Punkt 2.6 tiltak 21

Gruppen som skal være faglig støtte bør etter UiO sin oppfatning inkludere medlemmer som ikke kommer fra EOS. Dette av hensyn til en mer nøytral vurdering av såvel trusler og sikringsbehov, som av forskning og av spydspissteknologi.

Punkt 2.6 tiltak 22

UiO mener man bør vurdere å løsrive NorCERT fra NSM og la denne bli CSIRT for kritisk infrastruktur, samt opprette en ny paraply-CSIRT.

UiO anser NSM sin rolle til først og fremst å være ansvarlig og koordinerende. Det er noe uklart ved lesing av strategien i hvilken grad NSM ser for seg en rolle eller tilstedeværelse inne i eller foran IT-infrastrukturen til enkelte enheter innen forvaltningen. UiO er i utgangspunktet negativ til en slik tilstedeværelse, og mener at såvel sårbarheter som hendelser eller andre relevante initiativer bør gå fra enhetenes egne sikkerhetsorganisasjoner ut til NSM og at NSM ikke skal ha noen automatisk tilstedeværelse i enhetenes IT-infrastruktur.

Vedlegg A:

NorSIS har på papiret i dag en veilederrolle for mindre virksomheter samt for forvaltningen. UiO er usikker på om tilstrekkelig kapasitet og kompetanse eksisterer for å utøve denne rollen. UiO vil anbefale å innlede samarbeid med blant annet Akademia for å nyttiggjøre seg de ressursene som eksisterer der.

Generelt:

Strategien omtaler grenseflater mot de hemmelige tjenestene, Kripos med flere. I det daglige er imidlertid mye av problemene med IT-sikkerhet knyttet til helt alminnelig interaksjon mellom virksomheter hvis handlinger forhåpentligvis sjelden eller aldri faller innenfor disses domener og hvis infrastruktur kanskje ikke er kritisk.

Det finnes i det offentlige andre viktige normer og rammer som er svært relevante for IT-sikkerhet, for eksempel å kunne styre anbudsprosesser slik at det stilles tilstrekkelige krav når det gjelder IT-sikkerhet. Her kommer for eksempel DIFIs arkitekturprinsipper inn. Vi ønsker en klarere avklaring av roller og samhandling mellom NSM og DIFI hva angår IT-sikkerhet i det offentlige, særlig hva angår anskaffelser av nye systemer.

Med hilsen

Tove Kristin Karlsen
Assisterende direktør

Lars Inge Oftedal
IT-direktør

Lars Inge Oftedal
22852520 lars.oftedal@usit.uio.no