

IT-sikkerhet i det norske samfunn



- Litt om SIS
- Hva har vi sett
- Aktuelle trusler

Ove Olsen, SIS

Senter for informasjonssikring - SIS

- SIS er etablert som et prøveprosjekt etter avtale mellom Nærings- og handelsdepartementet og SINTEF Tele og data (STD).
- Prøveprosjektet varer fra 01.04.02 til 31.12.04.
- Oppdraget kan forlenges etter avtale.
- Prosjektet er et samarbeid mellom STD og UNINETT.

Senterets hovedoppgaver i forsøksperioden vil være:

- Å fremskaffe et helhetlig bilde av trusler som berører IKT-systemer i Norge.
- Formidle informasjon, kompetanse og kunnskap om trusler og mottiltak.
- Ha kontakt og samarbeid med tilsvarende organisasjoner i andre land.

SIS arbeidsform

- Motta informasjon fra inn- og utland.
 - hendelser
 - analyser, undersøkelser, rapporter
- Analysere hendelser og mottiltak.
- Gi tilbakemelding til de som rapporterer.
- Sende ut informasjon, både åpen og lukket, til inn- og utland.
- Kontakt og samarbeid med offentlige organer, organisasjoner og bedrifter i inn- og utland.

Informasjonsinnsamling

Etablerer kontakt med sentrale virksomheter i Norge:

- Finanssektoren
- Helsesektoren
- Energisektoren
- Olje og gass
- Politi
- Kommunikasjon
- Forsvarssektoren
- Offentlig forvaltning
- Forskning og utdanning
- Transport

Formell avtale regulerer utveksling av informasjon

Hva har vi sett så langt?

- Rammekrav
- Sikkerhetsledelse
- Styringssystem
- Ressursbruk til sikkerhet
- Overvåking
- Beredskap
- Samarbeidsfora

Rammekrav

- Mange kravdokumenter om sikkerhet.
- Hvert tilsyn har eget kravdokument.
- Bransjespesifikke.
- Lite koordinerte.
- Varierende bruk av internasjonale standarder.
- Kjennskap varierer.
- Kravdokument - må følges av kontrollrutiner.

Sikkerhetsledelse

- Sikkerhetsorganisasjon
 - Sikkerhetssjefens organisasjonsplassering
 - Ressurser
- Risikostyring
 - må inngå i ledelsesprosess
 - mangler verktøy
- Oppfølging av hendelser
 - hendelsesregistrering mangler
- Sikkerhetsopplæring

Styringssystem

- Sikkerhet må integreres i styringssystemet.
- Bruk av internasjonale standarder.
 - BS 7799/ISO 17799
 - COBIT
 - ISF - Standard of Good Practice
- Sertifisering:
 - Pr. dato er sju norske bedrifter sertifisert i hht. BS 7799.
 - Tre organisasjoner er akkreditert for sertifisering.

Overvåking

- Blir sikkerhetskrav etterlevd?
- Revisjoner
 - interne/eksterne
- Sikkerhetstester
- Inntrengingsdeteksjon (IDS)
 - Egen
 - Ekstern leverandør
 - VDI

Beredskap

- Incidence Response Team (IRT)
 - 24/7
 - Myndighet må tildeles.
- Katastrofeberedskapsplaner
 - Er disse kjent?
 - Er de oppdatert?
- Testing - omfang
- Vedlikehold

Samarbeidsfora

- Mange i Norge
- Bedrifter er medlem i flere sikkerhetsorganisasjoner
- Tordenskjolds soldater

Trusselbildet - utdrag

- Norge skiller seg ikke særlig ut fra resten av verden.
- Formell risikoanalyse mangler ofte i forkant.
- Med hele verden som lekegrind (Internett).
- Lite gjennomtenkt bruk av e-mail.
- Kompliserte systemer
 - påbygninger på mange plattformer
- Mange rettelser (patcher).
- Tyveri - bærbare enheter.



post@norsis.no

www.norsis.no