Vår saksbehandler	Vår dato	Vår referanse
Knut Lindelien / August Nilssen	2010-06-29	023.1
	Deres dato	Deres referanse
	2010-03-30	2010/00794-1/FD I 5/ODF

Forsvarsdept
0030 Oslo

Sendt pr epost til : postmottak@fd.dep.no

Høringsuttalelse fra Standard Norge om "Nasjonal strategi for Cybersikkerhet"

Standard Norge vil med denne høringsuttalelsen gi anerkjennelse til det arbeid som er utført i regi av NSM i samarbeid med Forsvarsdept og Justisdept. Vi vil i det følgende påpeke momenter som børe vurderes i det videre arbeidet.

Standarder

Standarder utviklet i de formelle internasjonale standardiseringsorganisasjonene ISO og CEN samt ETSI og ITU, innen områdene informasjonssikkerhet, IT-governance og risk management, har og vil fortsatt ha en vesentlig betydning for alle former for risikovurdering og tilhørende sikkerhetsvurderinger. Dette gjelder også for nasjonal- og global elektronisk kommunikasjon i og offentlig sektor så vel som i og privatsektor. Standard Norge deltar i dette internasjonale arbeidet.

Norsk ekspertdeltakelse i ulike arbeidsgrupper i ISO og CEN er imidlertid hemmet på grunn av manglende finansiering. Standard Norge anbefaler derfor at det avsettes finansielle resurser for norske ekspertdeltakelse i langt større grad enn hittil. Dette for å sikre bredest mulig deltakelse i dette viktig arbeidet fra så vel norske FoU miljøer, akademia, offentlig sektor og næringslivet.

Gjennom aktiv norsk deltakelse i standardiseringsaktivitetene i ISO og i CEN, vil våre nasjonale FoU miljøer og andre utvikler og brukermiljøer kunne hente og dele verdifull kunnskap for å vedlikeholde slik kompetanse i Norge.

Alle standarder som er utviklet i ISO eller CEN er tilgjengelige hos Standard Online på www.standard.no

Arbeidene foregår primært i :
ISO/IEC JTC 1/SC 27 IT Security techniques
Med følgende fokusområder:
JTC 1/SC 27/WG 1 Information security management systems
JTC 1/SC 27/WG 2 Cryptography and security mechanisms
JTC 1/SC 27/WG 3 Security evaluation criteria
JTC 1/SC 27/WG 4 Security controls and services
JTC 1/SC 27/WG 5 Identity management and privacy technologies

Postadresse
Standard Norge
Postboks 242
1326 Lysaker

Besøksadresse
Strandveien 18

Tel. 67 83 86 00
Faks 67 83 86 01

info@standard.no
www.standard.no

Bankkonto
1644 17 27384
Foretaksregisteret
NO 985 942 897

Det er også pågående arbeider i Europa i CENT C 225 Automatic Identification and Data Capture (AIDC) Technologies and Applications.

Bred norsk deltakelse i internasjonalt standardiseringsarbeid vil bidra til mer erfaring om hva som faktisk har vist seg gjennomførbart, om hva som oppfattes som problemer, om hva som er beste praksis og hva som meldes av hendelser (incidens) eventuelt fra ulike områder. Hovedgevinsten ved å delta i arbeiden i ISO er at vi får et bredere tilfang av kunnskap om hva som kan påvirke samfunnssikkerheten.

Når det gjelder ISO/IEC JTC 1SC27 WG4 er denne komiteen opptatt av å se på hvilke teknologiske muligheter som endrer på sikkerhetsutfordringene. Bakgrunnen er at nye teknologiske muligheter åpner nye risikoområder. Standardiseringens metodikk for å samle alle interessenter rundt konsensusløsninger og sjekke ut om standardene er gode nok over tid, bidrar i vesentlig grad til at standardene faktisk blir brukt.

Fra internasjonale studier kjenner Standard Norge til at et hovedproblem er at det i virksomhetene er få eller ofte ingen som har dedikert ansvar for sikkerhetsarbeidet. Bedrifter og organisasjoner med større grad av IT-avhengighet og avhengighet av IT-løsninger i nett og ”utenfor eget hus” vil være bedre stilt ved aktivt å bruke standarder som sikkerhetshjelpemidler. Avdekking og håndtering av risiko bør gjøres på et vis hvor det er ganske enkelt å finne ut om samarbeids- og forretningspartnere har omtrent samme metodikk som i egen organisasjon. Om alle virksomheter har sin egen metode blir det vanskelig å kunne lite på andre. Her hjelper standarder og i tillegg et system med sertifisering i henhold til standarder.

Standard Norge leser strategiforslaget som å være først og fremst rettet mot offentlig sektor. Dette blir etter vår mening alt for snevert og kan føre til mer fokus på hjemmelsgrunnlaget enn å se på hvilke egeninteresser virksomheter har/kan ha av bedre sikkerhetsarbeid. Det er også slik at investeringer og endringer i sikkerhetsarbeidet også må kunne rettferdiggjøres ut fra lønnsomhetsbetraktninger. Offentlige pålegg kan nok virke, men klare fakta om verdien av sikring vil antakeligvis også virke like godt eller bedre. Standard Norge vil derfor anbefale et langt sterkere fokus på næringslivets elektroniske samhandling med offentlig sektor i et globalt perspektiv.

Vi vil som eksempel også henlede oppmerksomheten på et workshop dokument fra amerikansk standardisering ISA/ANSIs (USA) :
” ISA/ANSIs The Financial Management of Cyber Risk”, er et dokument som gir et interessant grunnlag for det videre arbeid med den nasjonale strategien. Her fremgår det at hovedproblemet i forhold til ”Cybersikkerhet” er ikke angrep fra utenforstående, fiendtlige makter eller organisasjoner, men manglende rutiner og aktsomhet som fører til feil som gjøres av egne ansatte.

Rapporten peker også på at det er feil å legge ansvaret for ”cyber-security” hos IT-avdelingen. Det må være et totalansvar og den som ”eier” data må være opptatt av å sikre disse. Det er sjelden en IT-avdeling har ressurser eller posisjon til å være på rett sted for å forebygge, eller løse, hendelser som går på sikkerheten til vitale funksjoner i virksomheten.

Vi vil også henlede oppmerksomheten på standarden:
NS-ISO/IEC 38500:2008 Corporate governance of information technology.

”Cyber-security”

Begrepet ”cyber-security” benyttes, men kan noen ganger være litt vanskelig da det gir skinn av at dette er noe helt spesielt. Det er det knapt. I ISO/IEC er det vanlig å bruke ”Cyber security” som benevnelse både på arbeidet i ISO/IEC JTC 1 WG4 og på et av standardarbeidene under komiteen.

Standarden ISO/IEC 27032 sier:
”Cyber security standards are security standards which enable organizations to practice safe security techniques to minimize the number of successful cyber security attacks.

ISO/IEC 27002 provides best practice recommendations on information security management for use by those who are responsible for initiating, implementing or maintaining Information Security Management Systems (ISMS). Information security is defined within the standard in the context of the C-I-A triad: the preservation of confidentiality (ensuring that information is accessible only to those authorised to have access), integrity (safeguarding the accuracy and completeness of information and processing methods) and availability (ensuring that authorised users have access to information and associated assets when required).”

Andre oppgaver i WG 4 er;
- ICT Readiness for Business Continuity (27031),
- Network Security (27033),
- Application Security (27034),
- Information Security Incident Management (27035),
- Best Practice on the provision of the time-stamping service (TR 29149),
- Security of Outsourcing (27036),
- Guidelines for digital evidence (27037),
- Intrusion to Detection Systems (18043),
- Storage Security og
- ICT Supply Chain Security.

Andre deler av SC27 arbeider med Information Security management systems (ISMS)
- ISMS Overview and Vocabulary (27000)
- ISMS requirements (27001)
- ISM Code of practice (27002)
- IS Risk management (27005)
- ISMS auditing (27007)
- Guidance to Auditors on ISMS controls (27008)
- ISM guidelines for inter-sector communications (27010)
- Guidelines for Auditing Management Systems (19011) ikjke lead I SC27/WG 1
- Guidelines for the integrated implementation of ISO/IEC 27001 and ISO/IEC 2000-1 (27013)
- Information Security Governance (27014)
- ISMS for the Financial and Insurance Service Sectors (27015)
- ISM Economics
- Taxonomy

I tillegg har WG5 noen identitetsforvaltnings- og personvernstandarder i arbeid;
- Biometric Information Protection (24745)
- Framework for Identity Management (24760)
- Privacy Framework (29100)
- Privacy Reference Architecture (29101)
- I x eea Entity Autentication Assurance Framework (29115)

- A Framework for Access Management (29146)
- A Privacy Capability Maturity Model (29190)
- Requirements on relative anonymity with identity escrow – model for authentication and authorization using group signatures (29191)

Listen er ikke uttømmende, men gir et godt bilde av internasjonale standardiseringsarbeid på dette området og hvilke tema som behandles. Har departementet spørsmål til uttalelsen ta gjerne kontakt med oss.

Vi beklager sen oversendelse av vår uttalelse.

Med hilsen

Ivar Jachwitz
Viseadm. direktør
Standard Norge