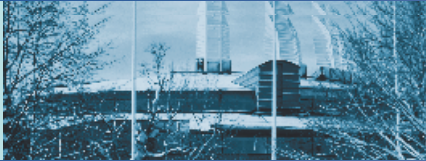


e-Stockholm'08

XXIII Nordic Conference on Law & IT
Aula Magna 17-19 November 2008



Juridik och informationssäkerhet

Helena Andersson
Krisberedskapsmyndigheten/Institutet för
rättsinformatik

Agenda

- Ett ömsesidigt beroende
- Informationssäkerhet - en juridisk uppgift
 - Session A
- Reglering av informationssäkerhet
 - Session B

Informationssäkerhet



- Säkerhetsskyddslagen (XX):
 - Konfidentialitetsskydd
 - Sekretessbelagd information
 - Rikets säkerhet
- Säkerhetsinformatik
 - Konfidentialitet
 - Riktighet
 - Tillgänglighet

Infosäkutredningen SOU XXX

Vår verktygslåda



- Teknik (brandväggar, antivirusprogram, IDS, BKS...)
- Organisatorisk (behörighetsadministration, informationssäkerhetspolicy, utbildning...)
- Etik (respekt för integritet...)
- Ekonomi (försäkringspremier, krav från handel ex PCI DSS)
- Juridik

Juridikens roll i informationssäkerhetsarbetet

- Ställa krav (personuppgiftslagen 31 §)
- Definiera (elektronisk signatur i lag om kvalificerade elektroniska signaturer)
- Peka ut ansvar (tillhandahållare av allmänt tillgängliga kommunikationsnät, personuppgiftsansvariga)
- Straffbelägga (dataintrång BrB 4:9c)

Juridiken - utmaningar



- Brist på systematik (samband, luckor)
- Holistiskt perspektiv (över rättsområden)
- Tvärdisciplinär samordning (teknik..)
- Terminologi (sekretess, integritet)
- Rörligt mål (snabb utveckling)
- Många aktörer
- Ej etablerad metod (ny reglering..)

- Behov av förändring?

Avhandlingen

- Ej traditionell uppgift
- Outforskat område
- Teknik/säkerhetsinformatik (nödvändig grund)
- Säkerhetsskyddslagens definition av informationssäkerhet (sekretessbelagt pga rikets säkerhet, konfidentialitetsskydd)
- Holistiskt – informationsinfrastrukturer (CIIP)
- Behov av metod - RISA

RISA Rättsinformatisk informationssäkerhetsanalys

- Mål: Att forma juridiken till ett ändamålsenligt säkerhetsverktyg
 - Systematik (samband)
 - Helhetssyn (gränsöverskridande)
 - Transparens (nåbarhet)
 - Pro-aktivitet
- Arbetsätt
 1. Definition av informationssäkerhet
 2. Kunskap och förståelse
 3. Strukturerat arbete

1. RISA Strukturering



- Identifiering:
 - Konfidentialitet, riktighet och tillgänglighet
- Vilket mål:
 - Fysisk säkerhet
 - Logisk säkerhet
 - Administrativ säkerhet
- Vilket medel:
 - Krav
 - Definition
 - Ansvar
 - Straffbeläggande

- Exempel – datainträng 4:9c BrB

2. RISA Relatering



- Rättslig reglering i en informationssäkerhetskontext
 1. Miljökartläggning
 2. Analys
 3. Identifierade brister (faktiska och teoretiska)
 - Luckor
 - Oklarheter

3. RISA Implementering



- 1. Vilka av bristerna i regleringen bör åtgärdas?
- 2. Ska bristen åtgärdas med rättsliga medel?
- 3. Hur ska en sådan reglering utformas?
- Checklista

Juridik och informationssäkerhetsspåret

- Session A: Informationssäkerhet - en juridisk uppgift:
 - Behovet av informationssäkerhet för att trygga mänskliga fri- och rättigheter, *Ahti Saarenpää, Institutet för rättsinformatik, Lapplands universitet*
 - Rättens roll i skyddet mot nätverksintrång, *Conny Larsson, Kronofogden, och André Rickardsson, Bitsec*
 - Digitale certifikater og certifikattjenester, *Rolf Riisnaes, Wikborg, Rein & Co*
 - Digitala bevis, *Stefan Kronqvist, Rikskriminalpolisen*
 - Paneldiskussion, *Per Furberg (moderator), Setterwalls*

Juridik och informationssäkerhetsspåret

- Session B: Reglering av informationssäkerhet
 - Information Security Regulations: Explaining Compliance and Non-Compliance, *Tommy Tranvik, NRCCL, Oslo universitet*
 - Föreskrifter om informationssäkerhet, *Wiggo Öberg, KBM*
 - Ledningssystem för informationssäkerhet, *Fredrik Björck, Visente*
 - En nationell handlingsplan för informationssäkerhet, *Per Oscarson, KBM*
 - Ett holistiskt perspektiv på informationssäkerhet, *Louise Yngström, DSV*
 - Paneldiskussion



Helena Andersson

Krisberedskapsmyndigheten

Helena.andersson@kbm-sema.se