Kontekst for sikkerhetssatsingen

Gustav Birkeland

Uninett workshop 14. januar 2019

Noe av konteksten for sikkerhetssatsingen:

- Risiko- og sårbarhetsbildet
- Egen vurdering og evaluering av sikkerhetstilstanden
- Riksrevisjonens kritikk
- Ny styringsmodell på sektornivå – forebyggende sikkerhet
- Rammeverk for håndtering av IKT-hendelser – konsekvensreduserende sikkerhet
- Ny personopplysningslov (GDPR)
- Ny nasjonal strategi for digital sikkerhet

Omtale av finansieringen i Prop. 1 S (2018-2019)

*For å styrke informasjonstryggleiken i universitets- og høgskolesektoren og betre evna til å **førebygge** og **handtere** truslar mot forskingsnettet, foreslår Kunnskapsdepartementet å løyve 17,5 mill. kroner til Direktoratet for IKT og fellestenester i høgre utdanning og forsking (UNIT) for å etablere eit program for informasjonstryggleik. Programmet vil i utgangspunktet gå over fire år og inneber ei rekke tiltak, mellom anna for betre **kapasitet** til å oppdage og handtere brot på informasjonstryggleiken, **analyseverktøy** og **kompetanseheving**.*

Et løft av sikkerheten er nødvendig for å lykkes med digitaliseringen

Jeg ønsker at virksomheter innenfor høyere utdanning og forskning skal ha et spesielt fokus på informasjonssikkerhet og personvern i arbeidet med å videreutvikle en kvalitetskultur. I digitaliseringsstrategien har derfor Kunnskapsdepartementet oppfordret institusjonene til å løfte informasjonssikkerheten høyere enn de nasjonale minstekravene for å være i stand til å gjennomføre en strategisk satsing på digitalisering. Samtidig har departementet satt som mål å styrke egen styring av informasjonssikkerhet på sektornivå gjennom et tydeligere rammeverk for hvordan denne styringen skal foregå.

Brev fra Forsknings- og høyere utdanningsministeren
om styringsmodellen 7. januar 2019

Styringsmodellen

- Basert på ISO/IEC 27014:2013 (…) Governance og information security
  - Generelle konsepter med mål og målbilder for styring av informasjonssikkerhet
  - 6 prinsipper for styringen
  - 5 prosesser som beskriver styringen
  - Rendyrket 'GRC' og kompatibel med andre styringsrammeverk for f.eks. IT-styring, risikostyring, økonomistyring mm.
  - Designet for virksomhetsnivået men anvendes nå av KD og Unit på sektornivået
  - Nivået over ISO/IEC 27001:2017, styring - ledelse

Prinsipper

1. Etablere informasjonssikkerhet som omfatter hele sektoren
2. Anta en risikobasert tilnærming
3. Gi retning til investeringsbeslutninger
4. Sikre etterlevelse av interne og eksterne krav
5. Skape et miljø som er positivt til sikkerhet
6. Vurdere gjennomføringsevne opp mot målbilder

Kort om noen sider av prosessene i modellen

1. Styre
   - Informasjonssikkerhetsstrategi og –policy, definere risikoaksept, tilpasse til sektormål, digitaliseringsstrategi, mm.
2. Monitorere
   - Risikovurdering på sektornivå mm.
3. Evaluere
   - Sikre at nye satsinger tar høyde for informasjonssikkerhet, evaluere måloppnåelse, korrigere mm.
4. Kommunisere
   - Kommunisere tilstand til interessenter, utvikle rammeverk og foreslå beste praksis, informasjons til sektoren ,mm.
5. Forsikre
   - Uavhengige evalueringer, revisjon