Kunnskapsdepartementet

Statlige universiteter og høyskolers ansvar for IKT-sikkerhet og digital hendelseshåndtering

Gustav Birkeland, seniorrådgiver

IRT: Nettverkssamling for hendelsesresponsteam i UH-sektoren, UNINETT fagsamling 20.11.2017

Departementets sektoransvar

- *"Kunnskapsdepartementets overordnede mål for arbeidet med samfunnssikkerhet og beredskap i kunnskapssektoren er å forebygge uønskede hendelser og minske konsekvensene av de hendelsene som likevel*

Fire grunnleggende prinsipper

1. Ansvarsprinsippet
2. Likhetsprinsippet
3. Nærhetsprinsippet
4. Samvirkeprinsippet

Forebygging og beredskap

- *Forebygging* handler om iverksetting av tiltak for å redusere sannsynligheten for en hendelse og for å redusere konsekvensene av en hendelse dersom den likevel inntreffer.
- Begrepet *beredskap* er definert som planlegging og forberedelser av tiltak for å begrense konsekvenser av uønskede hendelser og planer for å håndtere kriser eller andre uønskede hendelser på best mulig måte.

DSBs veileder Departementenes systematiske samfunnssikkerhets- og beredskapsarbeid.

- Departementet jobber både med forebygging og beredskap innenfor informasjonssikkerhetsområdet og da primært gjennom UNINETT.

KDs krav til statlige universiteter og høyskoler

- Styringsdokumentet skal ligge til grunn
- Skal utføre virksomhetstilpassede ROS-analyser minimum annet hvert år
- Skal ha oppdaterte krise- og beredskapsplaner og gjennomføre årlige kriseøvelser.
- Omfatter også informasjonssikkerhetsarbeidet
- Disse kravene gjelder også for virksomheter institusjonen har ansvar for, (f.eks. § 1.4.4-organer og eventuelle institutter i utlandet). Bør vurdere tilrettelegging overfor aksjeselskaper hvor institusjonen har over 50 prosent eierskap

Rapporteringskrav for sikkerhet og beredskap

1. Er det gjennomført/revidert en ROS-analyse, herunder også for informasjonssikkerhet, i 2016 eller 2017, og som er behandlet av styret?

2. Er det gjennomført og evaluert en kriseøvelse i 2017?

3. Redegjør for virksomhetens oppfølging av de fem tiltaksområdene i Handlingsplan for informasjonssikkerhet, herunder kort beskrive og

vurdere virksomhetens ledelsessystem for informasjonssikkerhet.

4. Ledelsessystem for informasjonssikkerhet: Er det innført en rutine for melding og håndtering av avvik og sikkerhetsbrudd (jf. også personopplysningsforskriften § 2-6), og er de viktigste avvikene behandlet i ledelsens gjennomgang?

Skal presentere forpliktende plan for det som ikke er fulgt opp.

Noen aktuelle nasjonale føringer

- Lovkrav: Personvernforordningen (GDPR)
- Justis- og beredskapsdepartementets stortingsmelding om IKT-sikkerhet:
  - Regjeringen er opptatt av å styrke vår nasjonale evne til å avdekke og håndtere digitale angrep.
  - Videre ønsker regjeringen å legge til rette for god informasjonsdeling og håndtering gjennom etablering og videreutvikling av nasjonalt rammeverk for digital hendelseshåndtering.
- Erfaringer fra øvelse IKT16
- Nasjonal strategi for informasjonssikkerhet

Digitaliseringsstrategi for universitets- og høyskolesektoren

- Strategi for å styrke evnen til å nå sektormålene til universitets- og høyskolesektoren gjennom en felles satsing på digitalisering
  - Høy kvalitet i utdanning og forskning
  - Forskning og utdanning for velferd, verdiskapning og omstilling
  - God tilgang til utdanning
  - Effektiv, mangfoldig og solid høyere utdanningssektor og forskningssystem
- En styrking av informasjonssikkerheten er en kritisk suksessfaktor for å klare denne satsingen.

Digital hendelseshåndtering er viktig på alle nivåer i UH-sektoren

- Grunnleggende ivaretakelse av sikkerheten til den enkelte og til virksomheten
- En del av den nasjonale beredskapen for IKT-hendelser
  - Det enkelte IRT-team og UNINETT CERT inngår i nasjonalt rammeverk for digital hendelseshåndtering
- En kritisk suksessfaktor for at den enkelte institusjon og sektoren som et hele skal nå sine mål gjennom digitalisering
- Etterlevelse av lover og krav på sektornivå, nasjonal nivå og EØS-nivå.