Kunnskapsdepartementet

Fra sikkerhetsledelse til handling – ambisjoner og forventninger

Gustav Birkeland, seniorrådgiver

UNINET-konferansen, 22.11.2017, sesjon 4

Forventninger

Statlige universiteter og høyskoler skal etterleve de nasjonale og sektorielle kravene til informasjonssikkerhet

Ambisjoner

Statlige universiteter og høyskoler skal se en strategisk *egeninteresse* i å strekke seg lenger enn de nasjonale og sektorielle *minstekravene* til informasjonssikkerhet fordi dette er et fundament for digitaliseringen av den enkelte virksomhet og en forutsetning for overordnet måloppnåelse.

Digitaliseringsstrategi for universitets- og høyskolesektoren:

5.4.10 En målrettet styrking av informasjonssikkerheten

(Forventninger)

"Kunnskapsdepartementet har overordnet ansvar for informasjonssikkerheten i UH-sektoren og vil fortsette å stille tydelige krav til institusjonene, og følge opp disse kravene gjennom styring og tilsyn. Disse kravene bygger på nasjonale regler og føringer og må forstås som minstekrav til informasjonssikkerhet.

Digitaliseringsstrategi for universitets- og høyskolesektoren:

5.4.10 En målrettet styrking av informasjonssikkerheten

(Ambisjoner)

Departementet legger vekt på at UH-institusjonene har et bevisst forhold til informasjonssikkerheten som en kritisk suksessfaktor for egne digitaliseringsstrategier og strategiske satsinger. Universitetene og høyskolene er kunnskapsvirksomheter hvor forvaltning og foredling av informasjon/data er en del av kjernevirksomheten. Å videreutvikle denne kjernevirksomheten gjennom en strategisk satsing på digitalisering innebærer også at institusjonene må ha et aktivt forhold til styringen av informasjonssikkerheten, og ha en egen strategisk interesse i å løfte denne høyere enn de nasjonale minstekravene."

Forventninger: Dette er noe dere *skal* gjøre

- Minstekrav som er like for alle statlig virksomheter. Disse følger av regelverk og av instrukser gitt i rundskriv og tildelingsbrev Eksempler er:
  - Følge kravene i digitaliseringsrundskrivet
  - Etterleve eforvaltningsforskriftens §15
  - Ha beredskapsplaner
  - Gjennomføre øvelser
- Det er ikke et målbilde, men en 'baseline'

Forventninger: Kravene er helt klare og kommuniseres i alle kanaler

- Lover
- Forskrifter
- Rundskriv
- Strategier
- Handlingsplaner
- Tildelingsbrev
- Etatsstyringsmøter med påfølgende skriftlig tilbakemelding
- Tilsyn med påfølgende skriftlig tilbakemelding
- **Revisjon**

Riksrevisjonens Dokument 1 (2017-2018):
Svakheter ved informasjonssikkerhet i statlige virksomheter

Riksrevisjonen har over flere år tatt opp vesentlige svakheter ved styringssystemer for informasjonssikkerhet i en rekke statlige virksomheter. Revisjonen for 2016 viser at dette fortsatt er et område med utfordringer, selv for store og dataintensive statlige virksomheter. Flere forhold er tatt opp med respektive virksomheter, mens svakheter ved informasjonssikkerheten i Oljedirektoratet, Statens Vegvesen og Skattedirektoratet er vurdert som vesentlige og derfor omtalt særskilt i Dokument 1 del II under det respektive departement.

Riksrevisjonens Dokument 1 (2017-2018):
Svakheter ved informasjonssikkerhet i statlige virksomheter

- Riksrevisjonen har over flere år tatt opp vesentlige svakheter ved styringssystemer for informasjonssikkerhet i en rekke statlige virksomheter. Revisjonen for 2016 viser at dette fortsatt er et område med utfordringer, selv for store og dataintensive statlige virksomheter. Flere forhold er tatt opp med respektive virksomheter, mens svakheter ved informasjonssikkerheten i Oljedirektoratet, Statens Vegvesen og Skattedirektoratet er vurdert som vesentlige og derfor omtalt særskilt i Dokument 1 del II under det respektive departement.
- **Kunne dette vært oss?**

Riksrevisjonens Dokument 1 (2017-2018):
Svakheter ved informasjonssikkerhet i statlige virksomheter

Ledelsen har ansvaret for informasjonssikkerheten i virksomheten. Styringssystemet skal være et verktøy for ledelsen til å oppnå et tilfredsstillende sikkerhetsnivå. Vesentlige forbedringer i informasjonssikkerheten krever kompetanse og et vedvarende systematisk arbeid i virksomhetene. Departementene har et særlig ansvar for sikkerheten innenfor eget område. Mangelfull styring og oppfølging av informasjonssikkerhet gir risiko for at sensitiv informasjon, også personopplysninger, kan komme på avveie og at viktige tjenester for samfunnet settes ut av funksjon. (…)

Riksrevisjonens Dokument 1 (2017-2018):
Svakheter ved informasjonssikkerhet i statlige virksomheter

(…) Dette skjer til tross for stor oppmerksomhet om uheldige hendelser, samt omtale i Riksrevisjonens dokument 1 over flere år. Den raske digitaliseringstakten bidrar til å gjøre kritiske samfunnsfunksjoner sårbare. Ulike aktører tar i bruk stadig mer avanserte metoder ved dataangrep på statlige virksomheter. Riksrevisjonen mener det er kritikkverdig at det fortsatt er virksomheter der det er vesentlige svakheter ved informasjonssikkerheten.

Ambisjoner

Målene er tydelige og oppfordringen er gitt

Ambisjoner: Den enkelte virksomhet velger å løfte informasjonssikkerheten over de nasjonale minstekravene som følge av egen strategi

- Utgangspunktet er en forståelse av egen kjernevirksomhet, mulighetene for utvikling og risikoen for disse verdiene.
- Dernest kommer minstekravene – baseline.
- Det er krevende å styrke et område mens resten av virksomheten skal effektiviseres.
- Nøkkelen til denne effektiviseringen ligger i digitalisering og en av nøklene til vellykket digitalisering er grunnleggende sikkerhet.
- Spørsmålet er ikke hva vi må gjøre i dag for å etterleve kravene fra KD, men hva vi må gjøre i morgen for å være konkurransedyktige på utdanning og forskning.

Gjennomføring av ambisjonen

- En grunnleggende forståelse av kjernevirksomheten og at informasjonssikkerheten er til for denne
- Et bevisst forhold til risikostyring på alle nivåer
- En forståelse av de andre virksomhetsstyringsprosessene og hvordan styring av informasjonssikkerhet henger sammen med disse
  - Alt bygger på de samme prinsippene for corporate governance og er kompatibelt
- Å bygge på egne styrker og samarbeid

Gjennomføring av minstekravene

- Ledelsen må være med og ta et ansvar for informasjonssikkerheten
- Vi er forbi implementeringsstadiet nå
- Utfordringen kan synes å være å få lukket kvalitetssirkelen i et ledelsessystem – altså å få integrert sikkerhetsledelsen i de andre ledelsesprosessene og årshjulet til virksomheten

Hva gjør regjeringen?

- Oppfølging av Lysneutvalget
- Stortingsmelding om IKT-sikkerhet
- Ny nasjonal strategi for informasjonssikkerhet
  - Ny handlingsplan for informasjonssikkerhet
- Evaluering av handlingsplan for informasjonssikkerhet i statsforvaltningen og status på informasjonssikkerhetsarbeidet

Hva gjør KD?

- En målrettet styrking av informasjonssikkerheten gjennom
  - Tydeligere rammeverk for egen styring og organisering
- En styrking av organiseringen på sektornivå gjennom tjenesteorganet
- Bygge videre på UNINETTs gode arbeid
- Kunnskapsgrunnlag gjennom ekstern evaluering

Hva gjør tjenesteorganet?

- Styring av informasjonssikkerhet blir en viktig oppgave
- Overtar viktig kompetanse fra UNINETT

Hva gjør UNINETT?

- Leverer sikkerhetstjenester til sektoren
- Drifter infrastrukturen og har UNINETT CERT, UH-sektorens responsmiljø

Hva gjør universitetene og høyskolene?

- Ruster seg til å møte morgendagens utfordringer og til å lede an i digitaliseringen av høyere utdanning og forskning