Vedlegg 1 – Utdrag fra Digdirs notat:

Et nasjonalt løft for informasjonssikkerhet i offentlig forvaltning (v0.9)

Sammendrag

Betydning for evne til å utføre oppgaver og levere tjenester

I vår moderne verden har informasjonsbehandling svært stor betydning for offentlige virksomheters oppgaveløsing. Informasjonssikkerhet handler om å sikre informasjonsbehandlingen i de oppgavene og tjenestene som offentlige virksomheter har ansvaret for. Digital sikkerhet og sikkerhet i digitale tjenester er en viktig del av dette.

Informasjonssikkerhetsbrudd kan få konsekvenser for virksomhetens leveranser, økonomi og evnen til å utføre oppgaver og yte tjenester. Det kan få følger for innbyggere og ansatte, andre virksomheter, samfunnsfunksjoner eller nasjonale sikkerhetsinteresser. Det er derfor en lang rekke regelverk som på ulikt vis stiller krav til informasjonssikkerheten.

Virksomhetenes selvstendige ansvar

Virksomhetene har et selvstendig ansvar for å styre risiko for sine oppgaver og tjenester, inkludert informasjonssikkerhet. Arbeidet med informasjonssikkerhet skal være risikobasert, med fleksibilitet og rom for tilpasning til en virksomhets størrelse, egenart og risiko. Dette skal gi tilstrekkelig og kostnadseffektiv informasjonssikkerhet for alle oppgaver og tjenester, inkludert digitale tjenester.

For å ivareta dette ansvaret styrer ledelsen informasjonssikkerhet som et ledd i det å styre virksomheten. De delene av styringen som har spesiell oppmerksomhet på informasjonssikkerhet, kan deles inn i to hoveddeler:

- Styringsaktiviteter
- Sikkerhetstiltak

Utfordringer og behov

Anbefalinger og veiledning om hvordan arbeidet med informasjonssikkerhet kan gjennomføres har vært tilgjengelig fra flere aktører i flere år. Det er likevel krevende for den enkelte virksomhet å ha tilstrekkelig informasjonssikkerhet, og ivareta forpliktelser fra alle regelverk.

Utfordringsbildet er sammensatt, og inkluderer blant annet:

- Virksomheter har svake eller manglende styringsaktiviteter
- Virksomheter mangler grunnleggende sikkerhetstiltak
- Virksomheter må til en viss grad gjøre de samme vurderingene
- Virksomheter har utilstrekkelig oversikt over informasjonsbehandlingen
- Virksomheter har mangelfull forvaltning av sikkerhetstiltak
- Arbeidet i virksomhetene er kompetansekrevende

- Arbeidet er ressurskrevende også utover behovet for kompetanse
- Det er krevende å undersøke om omfang av sikkerhetstiltak er tilstrekkelig
- Det er vanskelig å evaluere informasjonssikkerhet på tvers av virksomheter
- Det er utfordrende å bruke og følge opp tjenesteleverandører
- Manglende tillit mellom offentlige virksomheter kan være hinder for digitalisering
- Vanskelig å få til helhetlig tilnærming i styringen av virksomhetene
- Mangelfull og fragmentert regulering

Felles økosystem for nasjonal digital samhandling og tjenesteutvikling

Tjenester fra ulike virksomheter vil henge tettere sammen inn i de neste årene. Man er i stor grad avhengig av andre virksomheter, og at de har tilstrekkelig informasjonssikkerhet.

Virksomheter skal samarbeide, bygge sammenhengende tjenester og dele data i et felles økosystem for digital samhandling og tjenesteutvikling.

Felles utfordringer på informasjonssikkerhetsområdet har betydning for digitale tjenester, og for tjenestekjeder i felles økosystem. Når tjenester henger sammen, kan en hendelse i én virksomhet kan få direkte konsekvenser for tjenester hos andre virksomheter.

Når virksomheter skal utvikle og levere tjenester sammen, er det behov for samarbeid og samstyring for å håndtere risiko i tjenestekjeden. Slikt samarbeid vil inkludere samstyring av informasjonssikkerhet. Det er derfor viktig å se på hvordan rammebetingelsene kan legge til rette for dette på en god måte.

Strategisk utvikling de neste årene

Det er fortsatt behov for en styrket og mer helhetlig tilnærming til informasjonssikkerhet i forvaltningen. Både små og store virksomheter har utfordringer, og det virker som det går sakte fremover.[1] Det er behov for et taktskifte i arbeidet med informasjonssikkerhet i forvaltningen.

Vi mener det bør komme et nasjonalt løft for informasjonssikkerhet generelt, og digital sikkerhet spesielt. Det er nødvendig for at forvaltningen skal være i stand til løse oppgavene sine og levere tjenester i fremtiden.

Ved å bygge på det som allerede finnes, og tilføre noen nye elementer, kan vi etablere en tydeligere felles referanseramme for arbeidet med informasjonssikkerhet i offentlige virksomheter. Det kan inkludere tydelige anbefalinger om:

- Struktur og innhold for styringsaktiviteter
- Basisnivåer med sikkerhetstiltak
- Felles tiltaksbank med sikkerhetstiltak

[1] For eksempel basert på SSBs undersøkelser om sikkerhet i tilknytning til digitalisering og IKT: https://www.ssb.no/statbank/list/iktbruks

Mulige gevinster

Videre arbeid i denne retningen, med disse mulige tiltakene, kan blant annet bidra til:

- At det blir enklere å utvikle sammenhengende tjenester og dele data
- Mer kostnadseffektivt arbeid med informasjonssikkerhet
- Styrket grunnleggende sikkerhet på tvers av forvaltningen
- Mer effektivt grensesnitt mot tjenesteleverandørmarkedet
- Tydeligere rammer for tjenesteutvikling i felles økosystem

Mulige tiltak i forvaltningen

Mulige tiltak inkluderer å utvikle og etablere:

- en tydeligere felles referanseramme for arbeidet med informasjonssikkerhet
- en katalog med oppgaver/tjenester og informasjonstyper
- basisnivåer med sikkerhetstiltak
- felles tiltaksbank for forvaltningen
- felles normering av konsekvenskategorier og -nivåer
- spesialtilpassede basisnivåer

På sikt vil det også være relevant å se på muligheten for å få på plass en ny lov om informasjonssikkerhet for offentlig forvaltning.

Det er en del elementer som alle virksomheter trenger i gjennomføring av styringsaktiviteter, spesielt vurdering og håndtering av risiko. Selv om virksomheter følger anbefalinger om styringsaktivitetene[2], og benytter eksempler fra veiledning, så må de utforme og tilpasse disse elementene selv. Noen av disse elementene kan utformes sentralt og gjøres tilgjengelig slik at virksomhetene kan bruke dem direkte, eller gjøre mindre tilpasninger til sitt behov.

Oversikt over informasjonsbehandlingen og dens betydning

Man har behov for oversikt over oppgaver, tjenester og informasjonsbehandlingen i disse. Det kan lages en katalog med oversikt over oppgaver, informasjonstyper som behandles i dem, regelverksbestemmelser som er relevante for de ulike informasjonstypene, og et utgangspunkt for å anslå hvor store konsekvensene ved informasjonssikkerhetsbrudd kan bli. Et slikt halvfabrikat kan redusere omfanget av det som må gjøres i hver enkelt virksomhet, og effektivisere arbeidet med informasjonssikkerhet.

Basisnivåer

Grunnleggende sikkerhetstiltak kan samles i et eller flere basisnivåer. De kan danne utgangspunktet for virksomhetens valg av sikkerhetstiltak for oppgaver, tjenester eller informasjonssystemer. Det kan både effektivisere arbeidet i virksomhetene og bidra til å gi et mer felles, grunnleggende sikkerhetsnivå på tvers av forvaltningen.

Sikkerhetstiltak som skal inngå i basisnivåer bør være uttrekk fra en felles tiltaksbank.

[2] https://www.digdir.no/informasjonssikkerhet/styringsaktiviteter/3153

Tiltaksbank

Det finnes en rekke oversikter over sikkerhetstiltak som man kan vurdere å benytte for å redusere risikoer til et akseptabelt nivå. Ved å hente sikkerhetstiltak fra en tiltaksbank[3] trenger man ikke bruke mye tid og ressurser på å utforme disse selv. En felles tiltaksbank for offentlige forvaltning vil:

- gjøre det mulig å lage basisnivåer med sikkerhetstiltak fra tiltaksbanken
- fungere som en felles referanse for veiledning om sikkerhetstiltak, slik at det blir lett for brukere å se ulik veiledning i sammenheng
- fungere som felles referanse for tilsynsmyndigheter
- bidra til å øke evnen til samarbeid mellom virksomheter

Kategorier og nivåer av konsekvenser

Virksomhetene har behov for å estimere mulige konsekvenser ved informasjonssikkerhetsbrudd. Det brukes til å sortere oppgaver, tjenester eller informasjonssystemer for å prioritere ressursbruken på arbeidet med informasjonssikkerhet. Konsekvenser brukes også som et av flere elementer for å forstå og vurdere risiko. Som en del av det å anslå størrelse på risiko, så danner det grunnlag for prioritering av ressursbruk i arbeidet med å håndtere risiko.

En anbefaling om konsekvenskategorier og konsekvensnivåer som kan benyttes i styringsaktivitetene kan redusere arbeidsmengden i hver virksomhet og effektivisere arbeidet med informasjonssikkerhet. Det kan øke kvaliteten på vurderinger og bidra til at resultatene blir mer like på tvers av virksomheter. Det at konsekvenskategorier og -nivåer er gjenkjennbare på tvers av virksomheter vil kunne øke evnen til samarbeid og samstyring av risiko.

Sterke anbefalinger og tilhørende veiledning

Anbefalinger i en felles referanseramme må støttes opp med veiledning fra ulike aktører. Denne veiledningen eksisterer i stor grad allerede, men kan tilpasses slik at den refererer til hvilke elementer i den felles referanserammen det veiledes om i mer detalj. For eksempel vil en tematisk veileder fra NCSC[4] om hvordan en virksomhet kan beskytte seg mot utpressingsskadevare referere til hvilke sikkerhetstiltak fra tiltaksbanken som er spesielt aktuelle med tanke på den trusselen. På denne måten fungerer tiltaksbanken som en felles referanseramme for all veiledning om typer eller grupper av sikkerhetstiltak, eller detaljert veiledning om utforming og etablering av spesifikke sikkerhetstiltak.

Anbefalinger og tilhørende veiledning skal gjøre det enklere for virksomhetene å ivareta sitt ansvar. Det at ting gjøres mer likt og felles på tvers av forvaltningen kan styrke evnen til samarbeid og samstyring, og bidra til gjensidig tillit mellom tjenesteeiere som er avhengige av hverandre.

[3] https://www.digdir.no/informasjonssikkerhet/tiltaksbankar/3057
[4] Nasjonalt Cybersikkerhetssenter: https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/

Anbefalinger eller regulering

Konseptene bør utvikles som anbefalinger til virksomhetene. Dersom basisnivåer og felles tiltaksbank viser seg å være nyttige i norsk sammenheng, så vil de ha størst nytteverdi dersom de brukes av de fleste virksomhetene i forvaltningen. På sikt kan det være aktuelt å se på muligheten for å stille krav om bruken av disse.

Det kan være starten på en opprydning i dagens fragmenterte regelverk, med tanke på at like hensyn skal reguleres likt.

Viktige sammenhenger

Offentlige anskaffelser og skytjenester

Offentlige virksomheter må styre risiko for sine oppgaver og tjenester, dette gjelder også når de understøttes og gjennomføres ved bruk av anskaffelser, inkludert tjenester som inngår i informasjonsbehandlingen.

Det vil være fordeler med større grad av felles kravstilling til leverandørmarkedet.

Det kan være fornuftig at anbefalinger og krav rettes til de offentlige virksomhetene og oppgavene og tjenestene de skal levere. De relevante delene av kravene må ivaretas av tjenesteleverandører, alt etter innholdet i tjenesteleveransen. En sertifiseringsordning for skytjenester kan for eksempel bygges på de samme basisnivåene som er anbefalt å benytte for offentlige oppgaver og tjenester. Det kan organiseres slik at det blir tydelig ansvarsdeling mellom kunde og leverandør.

Personvern

Det er mange oppgaver og tjenester i offentlig forvaltning som behandler personopplysninger, og informasjonssikkerhet er viktig for å ivareta fysiske personers rettigheter og friheter når det behandles opplysninger om dem.

Det er mye å hente i å samkjøre arbeidet med informasjonssikkerhet og personvern for de oppgavene og tjenestene det gjelder.

Styringsaktiviteter kan ha samme struktur uavhengig av hva som skal styres[5]. Det vil likevel være ulike metoder i bruk, og forskjellige måter å gjennomføre deler av aktivitetene på.

En felles tiltaksbank kan inneholde både sikkerhetstiltak og personverntiltak. Det kan gjøre det enklere for virksomhetene å kombinere arbeidet med informasjonssikkerhet og personvern for oppgaver og tjenester som behandler personopplysninger.

[5] https://www.digdir.no/informasjonssikkerhet/helhetlig-styring-og-kontroll-av-informasjonssikkerhet/2284

Digitaliseringsdirektoratets anbefalinger om videre arbeid

Digitaliseringsdirektoratet anbefaler at det startes et arbeid for å utvikle en tydeligere felles referanseramme for arbeidet med informasjonssikkerhet i offentlige virksomheter.

Digitaliseringsdirektoratet anbefaler at det startes et arbeid for å utvikle og prøve ut de mulige tiltakene som er beskrevet i dette notatet. Dersom det skal ha full effekt, bør det tas sikte på at det etter hvert skal dekke hele forvaltningen. Under utvikling og utprøving vil det likevel være fornuftig å fokusere spesielt på å møte behovene til virksomheter med lav modenhet eller lite tilgang på nødvendige ressurser til arbeidet med informasjonssikkerhet. Kommunene har de samme eller svært likeartede oppgaver og tjenester, og det vil være naturlig å starte med noen av tiltakene der.

Digitaliseringsdirektoratet anbefaler at nye tiltak for forvaltningen utvikles i samarbeid mellom de sentrale myndighetsorganene som veileder virksomhetene om informasjonssikkerhet og styring og kontroll og et representativt utvalg virksomheter fra ulike forvaltningsnivåer.