En veileder fra UH-sky

Risiko- og sårbarhetsvurdering av skytjenester.

Innholdsfortegnelse

Innledning

Alle virksomheter er forpliktet til å gjennomføre risikovurderinger av informasjonssikkerheten i skyløsninger før disse tas i bruk. Med informasjonssikkerhet menes evnen til å forebygge, avdekke og håndtere hendelser som kan føre til brudd på personopplysningenes konfidensialitet, integritet eller tilgjengelighet.[1] Arbeidet med risikovurderinger er en viktig del av institusjonenes ledelsessystem for informasjonssikkerhet.[2]

Når risikovurderingen er gjennomført, er det viktig å iverksette tiltak som reduserer risikoen for hendelser med uakseptabel høy risiko. Dette beskrives ofte som risikohåndtering.

Risikovurderinger skal også gjennomføres ved endringer som kan ha betydning for informasjonssikkerheten. Endringer kan være at det tas i bruk nye underleverandører, det skjer endringer i driftsopplegget eller at funksjonaliteten i tjenesten endres eller utvides. Les mer om de regulatoriske krav til informasjonssikkerhet i Juridisk veileder for skytjenester.

Nye risikovurderinger av skytjenesten kan gjennomføres ved at tidligere vurderinger revideres og oppdateres.

Formål

I denne veilederen gjøres det rede for de viktigste uønskede hendelser som kan føre til brudd på informasjonssikkerheten ved bruk av skytjenester. Slike hendelser skal avdekkes og vurderes i risikovurderinger. Til slutt bør det utarbeides forslag til hvilke tiltak som bør iverksettes for å redusere risikoen (risikohåndtering).

I veilederen gis også et kort forslag til hvordan risikovurderinger kan planlegges og gjennomføres.

Målgruppe

Veilederen retter seg spesielt mot ansatte ved universiteter og høyskoler som har ansvaret for valg og forvaltning av skytjenester. Veilederen kan også være nyttig for alle som jobber med informasjonssikkerhet til daglig.

Veilederens oppbygging

I første del av veilederen presenteres et forslag til hvordan risikovurderinger av skytjenester kan planlegges og gjennomføres. I andre del drøftes de viktigste hovedområdene hvor uønskede hendelser kan oppstå. Til slutt i del 2 gis en oversikt over vanlige uønskede hendelser (brudd på informasjonssikkerheten) ved bruk av skytjenester.

Sekretariat for informasjonssikkerhet

Sekretariat for informasjonssikkerhet i UH-sektoren kan bistå institusjonene med planlegging og gjennomføring av risikovurderinger.

DEL 1: Planlegging og gjennomføring av risikovurderinger

I innledningen har vi nevnt at risikovurderinger skal gjennomføres før skytjenester tas i bruk. Risikovurderinger skal også gjennomføres ved endringer i skytjenesten som har betydning for informasjonssikkerheten.

---

[1] Konfidensialitet: Hindre uvedkommende i å få tilgang til informasjon.

Integritet: Hindre uautorisert endring og sletting av informasjon.

Tilgjengelighet: Sørge for at autoriserte personer får tilgang til informasjon, når de har behov for det.

[2] https://www.uninett.no/infosikkerhet/styringssystemer

I denne delen av veilederen gis en kortfattet innføring i hvordan risikovurderinger av skytjenester kan planlegges og gjennomføres.

Beslutningsgrunnlag

Risikovurderingen skal være en del av beslutningsgrunnlaget for om man skal anskaffe en skyløsning, og hvilken leverandør man eventuelt skal velge. Risiko som ligger utenfor akseptabelt nivå må håndteres gjennom risikoreduserende tiltak. Dette innebærer at institusjonen har en risikobasert tilnærming.

Som tidligere nevnt, er institusjonen juridisk forpliktet til å gjennomføre risikovurderinger. Se Juridisk veileder for skytjenester.

Utvelgelse av deltakere

Risikovurderingen foregår ved at man gjennomfører ett arbeidsmøte, hvor et utvalg deltakere diskuterer hvilke uønskede hendelser som kan skje ved bruk av skytjenester.

Sammensetningen av deltakerne er viktig. Det er viktig å samle et så bredt utvalg av type brukere som mulig, samtidig som man ikke bør være for mange. Sekretariatets erfaring er at det ikke bør være mer enn 8-10 deltakere. Det kan bli vanskelig å styre diskusjonen dersom det blir for mange.

Teknisk og brukerorientert ROS

Utvelgelse av deltakere til arbeidsmøtet kan være utfordrende fordi deltakernes kompetanse kan være svært ulik. Del derfor gjerne risikovurderingen inn i to deler. En for teknisk orienterte som har fokus på den tekniske delen av skyløsningen, og en gruppe som har fokus på bruk av løsningen sett fra sluttbrukernes ståsted.

Forberedende informasjon til deltakerne

Det er viktig at deltakerne får informasjon på forhånd som kan gjøre det lettere for dem å forberede seg på hva som skal risikovurderes. Her kan du finne eksempel på en slik forberedende informasjon med risikovurdering av Feide som eksempel.

Gjennomføring

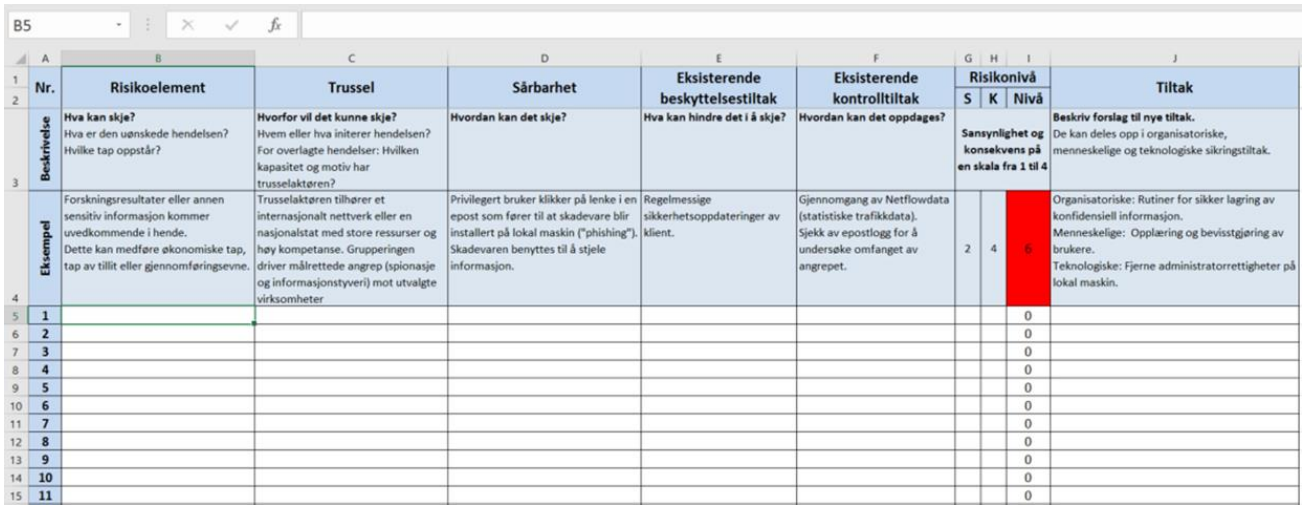
Arbeidsmøte må ledes av en fasilitator. Fasilitatorens rolle er å omskape diskusjonene i arbeidsmøtet til beskrivelser av mulige uønskede hendelser. Disse skal deltakerne deretter vurdere sannsynlighet og konsekvens for. Fasilitatoren bør på forhånd tenke igjennom hvilke risikoområder som bør drøftes i forbindelse med den aktuelle skyløsningen. Benytt gjerne hovedområdene og hendelsene som er beskrevet i denne veilederen. Del gjerne arbeidsmøte inn i tema slik som:

- Hendelser knyttet til brukerfeil
- Hendelser knyttet til forvaltning
- Hendelser knyttet til autentisering
- Hendelser knyttet til dataangrep
- …

På denne måten er det lettere å holde en struktur i arbeidsmøtet.

Når diskusjonen begynner å «gå i ring», det vil si at de samme hendelsene kommer opp igjen, er det på tide å avslutte denne delen av arbeidsmøtet.

Et eksempel på hvordan man kan registrere uønskede hendelser:



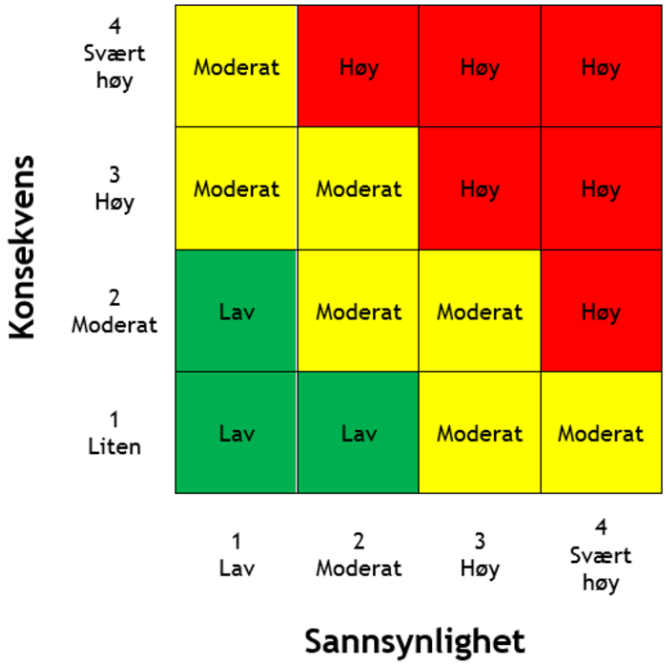
Nr.	Risikoelement	Trussel	Sårbarhet	Eksisterende beskyttelsestiltak	Eksisterende kontrolltiltak	Risikonivå S	Risikonivå K	Risikonivå Nivå	Tiltak
Beskrivelse	**Hva kan skje?** Hva er den uønskede hendelsen? Hvilke tap oppstår?	**Hvorfor vil det kunne skje?** Hvem eller hva initerer hendelsen? For overlagte hendelser: Hvilken kapasitet og motiv har trusselaktøren?	**Hvordan kan det skje?**	**Hva kan hindre det i å skje?**	**Hvordan kan det oppdages?**	**Sansynlighet og konsekvens på en skala fra 1 til 4**			**Beskriv forslag til nye tiltak.** De kan deles opp i organisatoriske, menneskelige og teknologiske sikringstiltak.
Eksempel	Forskningsresultater eller annen sensitiv informasjon kommer uvedkommende i hende. Dette kan medføre økonomiske tap, tap av tillit eller gjennomføringsevne.	Trusselaktøren tilhører et internasjonalt nettverk eller en nasjonalstat med store ressurser og høy kompetanse. Grupperingen driver målrettede angrep (spionasje og informasjonstyveri) mot utvalgte virksomheter	Privilegert bruker klikker på lenke i en epost som fører til at skadevare blir installert på lokal maskin ("phishing"). Skadevaren benyttes til å stjele informasjon.	Regelmessige sikkerhetsoppdateringer av klient.	Gjennomgang av Netflowdata (statistiske trafikkdata). Sjekk av epostlogg for å undersøke omfanget av angrepet.	2	4	8	Organisatoriske: Rutiner for sikker lagring av konfidensiell informasjon. Menneskelige: Opplæring og bevisstgjøring av brukere. Teknologiske: Fjerne administratorrettigheter på lokal maskin.
1								0	
2								0	
3								0	
4								0	
5								0	
6								0	
7								0	
8								0	
9								0	
10								0	
11								0	

Deretter skal deltakerne forsøke å gi en vurdering av 1) hvor sannsynlig det er at denne hendelsen inntreffer, og 2) hva er konsekvensen (skadevirkningen) dersom hendelsen inntreffer.

Eksempler på beskrivelse av verdier for sannsynlighet og konsekvens:

Konsekvens	Sannsynlighet
1 - Svært lite alvorlig Har ubetydelige skadevirkninger for enkeltpersoner eller NTNU som institusjon. Eksempel: Mangelfull logging av tilgang til personopplysninger; uklart når ikke-kritisk informasjon sist ble oppdatert; noe tapt arbeidstid.	1 - Svært lite sannsynlig Hendelsen kan skje sjeldnere enn hvert femte år.
2 - Mindre alvorlig Har visse skadevirkninger for enkeltpersoner eller NTNU som institusjon. Eksempel: Uautorisert eksponering av noen få personopplysninger; ufullstendig registrering av ikke-kritisk informasjon; informasjon er utilgjengelig opp til tre dager.	2 - Lite sannsynlighet Hendelsen kan skje sjeldnere enn hvert år, men oftere enn hvert femte år
3 - Alvorlig Har merkbare skadevirkninger for enkeltpersoner eller NTNU som institusjon. Eksempel: Uautorisert eksponering av sensitive eller større mengder alminnelige personopplysninger; viktig informasjon mangler eller er feil; informasjon er utilgjengelig opp til to uker.	3 - Sannsynlig Hendelsen kan skje hvert år.
4 - Svært alvorlig Har store skadevirkninger for enkeltpersoner eller NTNU som institusjon. Eksempel: Uautorisert eksponering av større mengder sensitive personopplysninger; kritisk informasjon mangler eller er feil; informasjon er utilgjengelig lengre enn to uker.	4 - Svært sannsynlig Hendelsen kan skje mange ganger i året.

Verdiene av sannsynlighet og konsekvens vil da utgjøre risikoverdien. Risikoverdien finner man ved å addere eller multiplisere verdiene for sannsynlighet og konsekvens. I figuren nedenfor illustrerer forholdet mellom de ulike verdier for sannsynlighet og konsekvens. Figuren viser om risikoen for en uønsket hendelse har blitt vurdert som høy, middels (moderat) eller lav.



Håndtering av risiko

Når institusjonen har gjennomført en risikovurdering har man avdekket hvilke uønskede hendelser som kan påvirke informasjonssikkerheten på en negativ måte. Det er særlig viktig at hendelser med høy risiko blir håndtert og at tiltak blir iverksatt for å redusere risikoen. Videre bør man gå igjennom de hendelsene som har middels høy risiko for å gjøre en vurdering av om institusjonen også her skal iverksette risikoreduserende tiltak.

I opplistingen av de mest vanlige uønskede hendelsene i denne veilederen, har vi kommet med forslag til hvilke tiltak som man kan gjennomføre for å redusere risikoen. Institusjonene må selv tenke igjennom om tiltakene er tilfredsstillende slik at risikoen reduseres til et akseptabelt nivå.

Dokumentasjon

Gjennomførte risikovurderinger og tiltak som etableres (risikohåndtering) skal dokumenteres skriftlig. Dokumentasjonen skal tas vare på.

Mer informasjon

Har du spørsmål om planlegging og gjennomføring av risikovurderinger, ta gjerne kontakt med Sekretariat for informasjonssikkerhet i UH-sektoren på infosec@uninett.no (alternativt kontakt@uninett.no).

DEL 2: Hovedområder og uønskede hendelser

Sekretariatet for informasjonssikkerhet har gjennomført en rekke risiko- og sårbarhetsvurderinger av ulike typer skytjenester. I disse risikovurderingene har sekretariatet avdekket en rekke uønskede hendelser som kan føre til brudd på informasjonssikkerheten.

Nedenfor følger en gjennomgang av de viktigste hovedområdene hvor uønskede hendelser kan oppstå. Senere i denne delen av veilederen gis en presentasjon av konkrete hendelser som kan oppstå innenfor disse hovedområdene. Se avsnitt om *«Uønskede hendelser som bør vurderes ved overgang til skyløsning»*.

Manglende styring og forvaltning av skytjenesten

Universitetet eller høgskolen må ha et bevisst forhold til hvordan skytjenesten skal styres og forvaltes. I dette ligger det at institusjonen må etablere et forvaltningsregime hvor ansvar og oppgaver med hensyn til informasjonssikkerheten i skyløsningen er tydeliggjort. Dette gjelder både internt på institusjonen og mellom leverandør og institusjon.

Forvaltningsregimet skal sette institusjonen i stand til å ivareta sitt ansvar som behandlingsansvarlig overfor sky-leverandøren som databehandler. Forvaltningsregimet er en del av institusjonens ledelsessystem for informasjonssikkerhet. Se sekretariatets veileder om ledelsessystem (www.uninett.no/infosikkerhet/styringssystemer).

Avhengighet til skyleverandør

Ved å ta i bruk skyløsninger er man ofte prisgitt leverandøren i langt større grad enn ved en lokal løsning. Det kan innebære lang responstiden når det gjelder feilrettinger og etablering av ønskede sikkerhetstiltak, og erfaringer indikerer at slike oppgaver kan ta lengre tid enn forventet. Det er derfor viktig med avtaler som regulerer responstiden på en tilfredsstillende måte.

Institusjonen bør anskaffe en skyløsning som gjør det enkelt å skifte skyleverandør dersom dette skulle bli aktuelt. Selv om det teknisk er mulig å skifte leverandør, kan migrasjons-tiden likevel bli lang. Institusjonen må også sørge for at forrige leverandør sletter data slik at disse ikke kommer på avveie.

Sikkerhetskopiering

Noen skyleverandører tar ikke tradisjonell sikkerhetskopi av dataene til sine kunder. Leverandørene benytter seg derimot av muligheten for å gjenskape data innenfor et gitt tidspunkt, for eksempel 90 dager. Data gjenskapes ved at skyleverandøren speiler eller replikerer data til flere lokasjoner. Dette medfører at disse leverandørene ikke kan gjenskape enkelt-filer eller data. Dersom man utilsiktet har slettet eller endret data i lagringsløsningen som man ønsker å få gjenskapt, er dette ofte problematisk.

Her må institusjonen vurdere behovet og eventuelt gå til anskaffelse av en tredjeparts sikkerhetskopieringsløsning. Denne vil i så fall kreve en egen risiko og sårbarhetsvurdering.

Manglende brukeropplæring

Selv om overgangen til en skyløsning ikke nødvendigvis medfører veldig stor forskjell på applikasjonene som benyttes, er det allikevel veldig viktig at brukerne har tilstrekkelig kompetanse om hvordan skyløsningen skiller seg fra lokal løsning. Skyløsningen vil innebære at data ikke lenger lagres lokalt, men ligger på en server ute i skyen. Dette gir store muligheter innenfor samarbeidsløsninger, slik som å kunne dele dokumenter internt eller eksternt. Men i neste omgang kan dette gi nye sikkerhetsutfordringer. Her må brukerne få tilstrekkelig opplæring slik at man ikke utilsiktet utleverer data som følge av manglende kompetanse om hvordan skyløsningen fungerer. En viktig utfordring i denne sammenhengen er at brukerne kan få mulighet til å gi eksterne brukere tilgang til institusjonens data. Uten tilfredsstillende opplæring, for eksempel å holde rede på tilgangslister, rettigheter, osv., kan dette føre til brudd på informasjonssikkerheten.

Driftspersonell må også få tilstrekkelig opplæring slik at man kan ivareta sikkerheten på en tilfredsstillende måte.

Manglende eller feil i dataisolasjon

En skyløsning innebærer at det er mange kunder (tenanter) som anvender samme fysiske maskin eller lagringsløsning. Selv om disse er adskilt logisk ved hjelp av virtuelle maskiner, kan feil i konfigurasjon, feil i administrasjonsgrensesnittet (hypervisor) eller menneskelig feil føre til at det oppstår datalekkasje mellom ulike kunder i løsningen. Det er derfor viktig å skaffe seg oversikt over hvordan skyleverandøren håndterer dette. Det er også viktig at skyløsningen gir tilgang til logger og monitoreringsdata slik at datalekkasjer oppdages og håndteres.

Organisatoriske endringer hos skyleverandør

Leverandører av skytjenester kan bli kjøpt opp eller fusjonert med andre aktører eller kan få økonomiske utfordringer. Dette kan føre til endringer hos skyleverandøren som påvirker kvaliteten på tjenesten, for eksempel nedbemanning, redusert kapasitet eller manglende sikkerhetsoppfølging. Derfor må institusjonen aktivt følge opp skyleverandøren for å tidlig avdekke svekket kvalitet på tjenesten, og følge opp dette med leverandøren. I denne forbindelse er det også viktig at institusjonen har mulighet til å skifte skyleverandør, eller selv overta driften av tjenesten. Se også punktet «*Avhengighet til skyleverandør*» over.

Manglende sletting av data

Når institusjonen ønsker permanent sletting av data, må man forsikre seg om at sletting blir gjort på en tilfredsstillende måte. På grunn av konseptet med et multitenant-miljø (mange kunder på samme løsning) og deling av maskinvare, er det ikke sikkert at data slettes tilstrekkelig eller fort nok slik institusjonen ønsker.

Det kan også oppstå sikkerhetsutfordringer når enkeltdisker i et lagringssystem skiftes ut på grunn av feil eller lignende, for eksempel pre-failure warranty.[3]

Manglende etterlevelse av lover og regler

Dagens regelverk stiller krav til informasjonssikkerheten og at institusjonen skal ha kontroll med egne data, se juridisk veileder for skytjenester. Dette medfører at man skal stille krav til en skyleverandør. Disse kravene omfatter blant annet at det inngås en databehandleravtale med skyleverandøren, og at institusjonen følger opp at avtalen overholdes. Se «Sjekkliste for databehandleravtaler i henhold til ny personvernlovgiving (GDPR)».

Å ivareta sitt rettslige ansvar innebærer også at institusjonen risikovurderer skyløsningen og at man gjennomgår revisjoner av informasjonssikkerheten hos skyleverandøren.

[3] Pre-failure warranty er et konsept som mange maskinvareleverandører tilbyr. Dette medfører at du får byttet en harddisk før den er defekt. Slike lesbare disker kan komme på avveier.

Uønskede hendelser som bør vurderes ved overgang til skyløsning

Under arbeidet med risikovurderinger i forbindelse med ulike skyløsninger har Sekretariat for informasjonssikkerhet skaffet seg erfaring med hva som er typiske uønskede hendelser. Dette avsnittet inneholder konkrete hendelser som kan påvirke informasjonssikkerheten på en negativ måte. Det pekes også på hvilke tiltak institusjonen kan iverksette for å redusere sannsynligheten for eller konsekvensen av at de inntreffer.

Hendelser som risikovurderinger i sektoren tidligere har blitt vurdert til høy og middels risiko, er tatt med i denne gjennomgangen. Hver enkelt institusjon må allikevel gjøre en selvstendig vurdering av risikoen for hver av hendelsene.

Hendelse 1:	Uvedkommende får tilgang til en annen brukers konto
Hva kan skje?	Data med behov for beskyttelse kan komme uvedkommende i hende. Dette kan for eksempel være sensitive personopplysninger, viktige bedriftshemmeligheter eller forskningsdata. Disse dataene kan også bli slettet, eller endret på uten at brukeren selv oppdager dette.
Årsak:	Dårlige holdninger ved at passord oppbevares på «gule» lapper eller ved at man blir utsatt for skadevare slik som en key-logger eller på annen måte blir frarøvet sine kontoopplysninger
Tiltak:	- Rutiner og opplæring på hva man kan legge ut i skyen. - To-faktor autentisering - Gjennomgang av logger og oppfølging av disse.
Antatt risiko:	HØY

Hendelse 2:	Feil tilgangsstyring til forskningsdata.
Hva kan skje?	I en skyløsning er det lett å dele forskningsdata med eksterne brukere. Skyløsningen er i utgangspunktet tilgjengelig fra internett, og dette åpner muligheten for å dele forskningsdata med eksterne brukere. Dersom man deler forskningsdata med feil ekstern bruker, eller glemmer å fjerne tilganger, kan data komme uvedkommende i hende.
Årsak:	- Menneskelig feil/svakhet - Manglende opplæring
Tiltak:	- Rutiner og opplæring på hva man kan legge ut i skyen. - Opplæring - Holdningsskapende arbeide - Gjennomgang av logger og oppfølging av disse.
Antatt risiko:	HØY

Hendelse 3:	Data er slettet, ingen sikkerhetskopi.
Hva kan skje?	Skyleverandører har ofte ikke sikkerhetskopiering slik som man er vant til fra lokale systemer. Noen leverandører kan gjenskape data på grunn av robusthet og redundans i sin løsning. Dette kan likevel føre til at enkelte data eller dokumenter ikke kan gjenskapes dersom de skulle bli slettet.
Årsak:	Skyleverandører opererer med at man for eksempel kan gjenskape data som er opptil 90 dager gamle. Dette kan av og til oppfattes som tradisjonell sikkerhetskopiering. Dermed kan man stå i fare for å miste data som det ikke finnes sikkerhetskopier av.
Tiltak:	- Gå til anskaffelse av tredjeparts sikkerhetskopieringsløsning.
Antatt risiko:	HØY

Hendelse 4:	Dataangrep mot løsningen blir ikke stoppet i tide
Hva kan skje?	Når institusjonen benytter en skyleverandør er man ofte avhengig av å få leverandøren til å gjøre mottiltak mot dataangrep. Dette gjelder spesielt dersom man er utsatt for et DDOS-angrep (distribuert tjenestenektangrep) eller «Phishing» kampanje. Institusjonen kan oppleve at responstiden fra leverandørens side i slike saker er utilfredsstillende lang. Et slikt sikkerhetsbrudd kan dermed bli mer omfattende enn nødvendig.
Årsak:	Institusjonen blir ikke prioritert av leverandøren.
Tiltak:	- Inngå avtale om responstid - Perimetersikring, logging, monitorering - Penetrasjonstest - SLA bør inneholde sanksjoner ved brudd - Undersøke muligheten for å benytte egen management-server hos skyleverandør slik at man kan håndtere hendelsen selv.
Antatt risiko:	HØY

Hendelse 5:	Utilfredsstillende sikring av data.
Hva kan skje?	Data som skulle vært særskilt beskyttet blir lagt i mapper på skyløsningen, hvor brukere uten tjenstlig behov får tilgang til disse dataene. Dataene kan dermed bli utlevert, endret eller slettet av uvedkommende.
Årsak:	Manglende klassifisering av data kan være en årsak. Andre årsaker kan være mangelfull oversikt over eller manglende rutiner for hvor ulike type data skal lagres, manglende brukeropplæring eller uklart dataeierskap.
Tiltak:	- Etablere og innføre klassifisering av data - Sørge for tilstrekkelig opplæring - Etablering av rutiner for håndtering av data, spesielt hvordan man skal håndtere data som er klassifisert som sensitive, viktige eller kritiske - Etablere rutiner for hvor ulike type data skal lagres
Antatt risiko:	HØY

Hendelse 6:	Lokale sikkerhetsbehov blir ikke ivaretatt
Hva kan skje?	Institusjonen klarer ikke å etablere tilsvarende sikkerhetsarkitektur som man tidligere hadde lokalt. Skyleveransen har en standardisert løsning som ikke har like gode muligheter for tilpasning til lokale sikkerhetsbehov. Dette kan føre til at institusjonens krav til sikkerhet ikke ivaretas av skyløsningen.
Årsak:	Manglende planlegging kan gjøre at institusjonen ikke sjekker ut hvorvidt det er mulig å gjenskape et sikkerhetsregime i henhold til institusjonens behov. Dette kan for eksempel skje ved at epostfilteret hos leverandøren ikke stopper skadelig epost, eller at epost som skulle vært levert blir stoppet av løsningen til leverandøren. Det kan også være nettverkskonfigurasjoner som ikke lar seg løse på tilsvarende måte i skyløsningen. Dette kan føre til at institusjonen blir utsatt for skadevare, eller dataangrep.
Tiltak:	- Tilstrekkelig planlegging og utsjekking mot leverandør før bestilling - Sørge for tilstrekkelige økonomiske rammer slik at man eventuelt kan oppgradere løsningen hos leverandøren for å dekke sine lokale behov - Test av løsningen før produksjon
Antatt risiko:	HØY

Hendelse 7:	Data blir lagret på usikre lokasjoner.
Hva kan skje?	Institusjonens data blir lagret på servere i land hvor man ikke har kontroll med sikkerheten.
Årsak:	Skyleverandøren kan benytter seg av datasentre i mange ulike land. Det kan være vanskelig for institusjonen å forsikre seg om at sikkerheten i disse datasentrene er tilfredsstillende.
Tiltak:	- Kunnskap om skyleverandørens datalokasjoner - Regulering av datalokasjon i databehandleravtalen - Kontroll med skyleverandørens underleverandører - Risikovurdering av skyløsningen
Antatt risiko:	HØY

Hendelse 8:	Data utilgjengelig, systemene virker ikke som forutsatt (IaaS).
Hva kan skje?	Ved en overgang til skyløsning virker ikke systemene som forutsatt. Dette kan føre til at data er utilgjengelige eller ufullstendige.
Årsak:	Noen applikasjoner er ikke utformet for en skyløsning (eldre applikasjoner). Disse kan fungere utmerket i et lokalnettverk, men man kan få problemer med for eksempel forsinkelser eller lignende når de flyttes ut i skyen. Dette kan føre til mangelfull tilgang til data.
Tiltak:	- Test av funksjonalitet i skyløsning i samarbeid med leverandør før beslutning tas - God planlegging ved overgang til skyløsning - Sjekk av referanser, andre som benytter samme applikasjon i skyen.
Antatt risiko:	MIDDELS

Hendelse 9:	Sikkerhetsbrudd ved utnyttelse av sårbarheter i systemer.
Hva kan skje?	Dersom nødvendige sikkerhetsoppdateringer ikke blir utført, kan institusjonens skyløsning bli utsatt for dataangrep. Denne sårbarheten kan utnyttes av interne, eksterne eller andre tenanter i samme «rigg» (installasjon).
Årsak:	Når institusjonen setter ut sine datasystemer i skyen må man allikevel sørge for at sikkerhetsoppdateringer blir utført. Ved bruk av skyløsninger kan det variere hvem som har ansvar for sikkerhetsoppdatering av systemene. Denne ansvarsdelingen må være tydelig. Dersom ansvarsfordelingen er uklar, kan det føre til at kjente sårbarheter blir utnyttet.
Tiltak:	- Inngå avtaler som tydelig beskriver hvem som har ansvar for hva - Jevnlig kontroll av at sikkerhetsoppdateringer er gjennomført - Gjennomføre sårbarhetsscanning
Antatt risiko:	MIDDELS

Hendelse 10:	Manglende mulighet til å oppdage sikkerhetsbrudd.
Hva kan skje?	Vanligvis tilbyr skyleverandører logger på applikasjonsnivå. Dette er ofte ikke tilstrekkelig for å avdekke konsekvensen ved et sikkerhetsbrudd. Dette medfører også at responsmiljøet (IRT) hos institusjonen ikke vil kunne avdekke mistenkelig trafikk eller angrep på nettverksnivå.
Årsak:	Årsaken til dette er ofte at skyleverandørene ikke ønsker eller ikke har kapasitet til å filtrere rådata (nettverksdata) som vil tilhører hver enkelt kunde.
Tiltak:	- Kreve å få tilgang til rådata (nettverksdata) som tilhører din institusjon.
Antatt risiko:	MIDDELS

Hendelse 11:	Data er utilgjengelige i skyløsningen.
Hva kan skje?	Dersom skyleverandører må gjøre endringer i eller ta ned deler av systemet for å gjøre feilretting hos enkelte av sine kunder, kan dette også påvirke tjenestekvaliteten på de øvrige kundene. Dette kan blant annet føre til at institusjonens data er utilgjengelige over en kortere eller lengre periode.
Årsak:	Behovet for stordriftsfordeler fører til komplekse skyløsninger. Dersom leverandøren ikke har full oversikt over kompleksiteten, kan det hende at flere kunder enn planlagt og varslet blir berørt.
Tiltak:	- Leverandøren må støtte «live migrering» - SLA som stiller krav til nødvendig oppetid
Antatt risiko:	MIDDELS

Hendelse 12:	Utilfredsstillende datatilgang.
Hva kan skje?	Dersom institusjonen ikke stiller tilstrekkelige krav til kapasiteten i skyløsningen, kan man oppleve at løsningen ikke skalerer i henhold til behov. Dette kan føre til utilfredsstillende tilgjengelighet eller treg tilgang til egne data i løsningen.
Årsak:	Mangelfull planlegging eller manglende kjennskap til ressursbehov ved bestilling av skyløsning. Dette kan også skyldes manglende rådføring med teknisk kompetent personell.
Tiltak:	- God planlegging hvor teknisk personell blir en del av anskaffelsesprosjektet
Antatt risiko:	MIDDELS

Hendelse 13:	Data blir avlyttet under transport til/fra skyleverandør.
Hva kan skje?	Kommunikasjon mellom skyleverandøren og institusjonen går via internettet. Dette fører til at datatrafikken kan avlyttes av uvedkommende. Tidligere var dette ikke et problem da datatrafikken gikk internt.
Årsak:	Manglende kunnskap og ubetenksomhet ved flytting av data
Tiltak:	- Kryptering av data i bevegelse
Antatt risiko:	MIDDELS

Hendelse 14:	Data på avveier som følge av datalekkasje mellom tenanter (kunder).
Hva kan skje?	Administrasjonsprogrammet (hypervisor) blir utsatt for et angrep eller en feilkonfigurasjon. Dette kan føre til datalekkasje mellom tenanter (kunder). Dermed kan sensitive eller kritiske data komme uvedkommende i hende.
Årsak:	Manglende sikkerhetsoppdatering av hypervisor/administrasjonsprogram eller manglende kompetanse eller kontrollrutiner på endringer.
Tiltak:	- Kryptere data under lagring - Stille krav til leverandøren om endringshåndtering - Stille krav til umiddelbar varsling ved slike hendelser
Antatt risiko:	MIDDELS

Hendelse 15:	Hele skyløsningen er utilgjengelig over tid.
Hva kan skje?	Skyleverandøren kan bli utsatt for ytre påvirkning som naturkatastrofer, brann, terror eller andre alvorlige hendelser. Dette kan føre til at hele skyløsningen blir utilgjengelig over tid.
Årsak:	Skyleverandøren har ingen kontinuitetsplan som er øvet og testet, og er dermed ikke i stand til å levere sine tjenester ved en katastrofelignende hendelse.
Tiltak:	- Kreve at leverandøren har oppdaterte kontinuitetsplaner - At leverandøren jevnlig har katastrofeøvelser - Leverandøren gjennomgår kontinuitetsplanene jevnlig - Etablere tredjeparts backup fra annen geografisk lokasjon
Antatt risiko:	MIDDELS

Hendelse 16:	Data kommer uvedkommende i hende på grunn av beslag fra myndigheter/politi
Hva kan skje?	Dersom en annen kunde hos skyleverandøren driver med kriminell virksomhet kan institusjonen oppleve at vedkommende kundes politimyndighet vil kreve beslag av data. Ved et beslag, spesielt dersom myndighetene krever å få utlevert fysiske lagringsmedium, kan institusjonens data også bli utlevert.
Årsak:	Skyløsningskonseptet er basert på stordriftsfordeler. Dette betyr at mange kunder deler prosessorkraft, minne og lagringsplass. Data spinner over i hverandre og deles logisk med det som kalles virtuelle maskiner. Dermed kan det være vanskelig å isolere data for en bestemt kunde (tenant).
Tiltak:	- Kryptering av lagrede data
Antatt risiko:	MIDDELS

Hendelse 17:	Uforutsette økonomiske tap
Hva kan skje?	Dersom institusjonen blir utsatt for et DDOS-angrep (tjenestenektangrep) vil dette kunne føre til at kapasiteten på institusjonens maskiner fylles opp slik at maskinene ikke lenger kan svare på legitime forespørsler. Systemet blir utilgjengelig og samtidig kan hendelsen føre til økonomiske tap.
Årsak:	Tapene kan skyldes at lisensieringen er slik at institusjonen må betale for de ressursene som til enhver tid benyttes (PAYG: Pay As You Go).
Tiltak:	- Avtal med leverandøren hvordan slike hendelser blir håndtert - Still krav om å bli varslet dersom leverandøren merker unormalt økt ressursbruk - DDOS-beskyttelse
Antatt risiko:	MIDDELS

Andre uønskede hendelser

Andre uønskede hendelser som har blitt avdekket under tidligere risikovurderinger av informasjonssikkerheten ved bruk av skytjenester diskuteres nedenfor. Selv om disse hendelsene har vært vurdert med lav risiko, må likevel din institusjon gjøre en selvstendig vurdering av disse hendelsene.

Hendelse 18:	Sikkerhetsbrudd som følge av inkompatibilitet med skyløsning
Hva kan skje?	Applikasjoner som driftes lokalt, er ofte integrert med hverandre. Når disse applikasjonene settes ut i en skyløsning, kan det tenkes at integrasjonene ikke virker slik de skal. Data kan da bli utilgjengelig eller løsningen kan bli ustabil. Det kan også innebære at brukerne mister tillit til skyløsningen.
Årsak:	Dårlig planlegging, testing eller mangelfull oversikt over sammenhenger i lokale applikasjoner.
Tiltak:	- Løsningen må testes grundig før migrering. - God planlegging og kartlegging av systemer, dataflyt og integrasjoner - Sørge for tilstrekkelig kompetanse i migreringsprosjektet
Antatt risiko:	LAV

Hendelse 19:	Utro tjener hos skyleverandøren
Hva kan skje?	Utro tjener hos skyleverandøren skaffer seg tilgang til institusjonens data. Den utro tjeneren har rettigheter til å kopiere, endre eller slette data. Dette kan føre til utlevering, uautorisert endre eller slette data.
Årsak:	En utro tjener hos skyleverandøren benytter seg av sine tilganger til for eksempel å selge data, personlister, eposter eller annen informasjon for egen vinnings skyld. Motivet for disse handlingene kan også være politisk eller ideologisk.
Tiltak:	- Kryptering av data hvor institusjonen har kontroll med krypteringsnøkkelen
Antatt risiko:	LAV

Hendelse 20:	Manglende styring av brukertilganger.
Hva kan skje?	Brukertilganger blir ikke endret eller avsluttet når personer (interne eller eksterne) skifter rolle, slutter eller av andre årsaker ikke lenger skal ha tilgang til data. Disse dataene kan dermed komme uvedkommende i hende.
Årsak:	Brukerne kan i stor grad i en skyløsning tildele andre brukere rettigheter inn til et område. Ved brukerfeil eller manglende oppfølging av tilgangslister som brukeren selv har ansvar for, kan uvedkommende ha tilgang til opplysninger denne ikke skulle hatt.
Tiltak:	- Opplæring - Jevnlig oppfølging av tilgangsrettigheter - Innføre tekniske løsninger som ikke gjør det mulig å dele områder med særskilt behov for beskyttelse. - Monitorering/logger
Antatt risiko:	LAV

Hendelse 21:	Brudd på tilgjengelighet av informasjon
Hva kan skje?	Skyleverandøren vil av og til ha behov for å oppgradere sine systemer. Det kan føre til at skyløsningen ikke er tilgjengelig for institusjonen. Ved kritiske oppgraderinger vil institusjonen vanligvis ikke bli varslet om nedetid. I noen perioder, for eksempel ved studiestart, kan dette være problematisk.
Årsak:	Mangelfulle eller uklare varslingsrutiner fra skyleverandørens side.
Tiltak:	- Varslingsrutiner må klart fremgå i en SLA, og være i henhold til institusjonens behov - Vurdere om kritiske systemer skal være en del av skyløsningen
Antatt risiko:	LAV

Hendelse 22:	Skyløsningen utsettes for dataangrep
Hva kan skje?	Skyleverandøren kan bli utsatt for et massivt dataangrep, for eksempel et distribuert tjenestenektangrep (DDOS).
Årsak:	Store skyleverandører har mange ulike kunder, og er dermed et fristende angrepsmål. Et angrep rettet mot en bestemt kunde kan også ramme øvrige kunder hos skyleverandøren. Dette kan føre til at skyløsningen blir utilgjengelig for institusjonen.
Tiltak:	- Forsikre seg om at skyleverandøren har løsninger som effektivt overvåker og kan håndterer dataangrep - Kreve at leverandøren har kontinuitetsplaner som er oppdaterte og testes jevnlig - Sette seg inn i og vurdere skyleverandørens løsning for å håndtere dataangrep
Antatt risiko:	LAV

Hendelse 23:	Uautorisert tilgang til data via felles-pc (internettkafé).
Hva kan skje?	En skyløsning er tilgjengelig via internettet. Uvedkommende kan få tilgang til skyløsningen dersom en bruker har benyttet en felles-pc (internettkafé).
Årsak:	En bruker har glemt å logge seg helt ut av skyløsningen. Dermed kan neste bruker trykker «tilbake» på nettleseren og få tilgang til forrige brukers data. En felles-pc kan også ha installert tastaturloggere som kan plukke opp brukernavn og passord.
Tiltak:	- 2-faktor autentisering - Opplæring/rutiner for bruk av felles-pc
Antatt risiko:	LAV

Hendelse 24:	Bruk av uautoriserte skyløsninger til lagring av institusjonens data.
Hva kan skje?	Brukeren benytter sin egen skyløsning til å lagre institusjonens data (for eksempel privat epost eller lagringsløsning). Dersom brukerens egen skyløsning har et lavere sikkerhetsnivå enn hva institusjonen tillater, kan dette føre til uautorisert tilgang til institusjonens data.
Årsak:	Skyløsninger har ofte mulighet for synkronisering av data til brukerens egen skyløsning. Uautorisert tilgang til institusjonens data kan for eksempel skyldes feil i oppsett av synkroniseringstjenesten eller innebygd automatikk i synkroniseringen.
Tiltak:	- Etablere løsninger som ikke gjør det mulig å synkronisere data mot andre ikke-godkjente skyløsninger - Etablere rutiner for bruk av skyløsningen - Opplæring av brukerne
Antatt risiko:	LAV

Mer informasjon

Du kan også finne mye nyttig informasjon på sekretariatets informasjonssider:
www.uninett.no/infosikkerhet

Informasjon om UNINETTs Sky program finner du på: www.uninett.no/sky