RAPPORT

Risiko- og sårbarhetsvurdering av Office365 skyløsning

Dato for gjennomføring: 24.05.2016 – 08.03.2017.

Til:	Institusjoner i UH sektoren
Fra:	Rolf Sture Normann
Forfatter:	Rolf Sture Normann
Kopi:	Tommy Tranvik
Dato:	31.05.2017
Gjelder:	ROS Office365

Innholdsfortegnelse

Forord 3
Innledning 4
Bakgrunn 4
Dokumentreferanser: 5
Gjennomføring 5
Arbeidsmøter (workshops) 6
Arbeidsmøte 8
Metodikk 9
Risikorapport 9
Rapportens oppbygning 9
Del 1: Hovedfunn – oversikt 11
Alle hendelser 11
Hendelser med høy risiko (risikoverdi 6 eller høyere) 11
Hendelser med middels høy risiko (risikoverdi 5) 11
Hovedinntrykk og overordnede risikoområder 12
Del 2: Hendelser med høy risiko og anbefalte tiltak – fokus på Sharepoint, teamsites og OneDrive . 15
Del 2: Hendelser med høy risiko og anbefalte tiltak – fokus på Exchange Online 18
Del 3: Tiltaksprioritering 24
Vedlegg 1: Risikomatrise – Arbeidsmøte 1, Sharpoint, teamsites og OneDrive 25
Vedlegg 2: Risikomatrise – Arbeidsmøte 2, Exchange Online 26
Vedlegg 3: Utklipp av utfylt regneark til denne rapporten 27
1. arbeidsmøte 27
Vedlegg 4: Melding til deltakerne i risiko- og sårbarhetsvurderingen – 1. arbeidsmøte 28
Vedlegg 5: Melding til deltakerne i risiko- og sårbarhetsvurderingen – 2. arbeidsmøte 30

Forord

Risiko- og sårbarhetsvurderingen av Office 365 skyløsning ved institusjon ble tilrettelagt av Sekretariatet for informasjonssikkerhet i UH-sektoren.

Sekretariat for informasjonssikkerhet i UH-sektoren er opprettet av Kunnskapsdepartementet og lagt til UNINETT AS.
I mandatet fra KD står det følgende om risiko- og sårbarhetsvurderinger:

«***Risiko og sårbarhetsvurderinger***
Sekretariatet skal tilrettelegge for risiko- og sårbarhetsvurderinger for enkeltinstitusjoner, og formidle erfaringer fra hele sektoren.»

Innledning

Bakgrunn

Institusjonen benytter i dag en hybrid skyløsning for Office365. Dette innebærer at en del av løsningen inkludert drift og data, ligger lokalt hos institusjonen, mens endel av løsningen ligger hos Microsoft. Når det gjelder epost og kalender er det kun studentene som er flyttet over på skyløsningen til Microsoft (Exchange Online). Ansatte hos institusjonen har fremdeles sin epost og kalenderløsning lokalt. Når det gjelder SharePoint, TeamSite og OneDrive benytter de ansatte Office365 som ligger i skyen. Dette medfører at delte dokumenter/data med interne eller eksterne aktører ligger hos Microsoft.
Det er et ønske fra institusjonens side å vurdere om også epost og kalenderløsningen (Exchange Online) kan gjelde alle brukere hos institusjonen, ikke bare studentene.

Noen av hendelsene som kom frem under arbeidsmøtene vil også gjelde dagens hybride løsning. Det er viktig å understreke at verdiene for sannsynlighet og konsekvens (skala 1-4) er vurdert ut fra at de ligger i skyen, hos Microsoft.

Før institusjonen gjør en endelig beslutning på dette, ønsker de å legge til grunn en risiko- og sårbarhetsvurdering for informasjonssikkerhet ved bruk og drift av Microsoft Office 365. Denne rapporten er et resultat av dette.

Risiko- og sårbarhetsanalysen er gjort i samarbeid med UNINETTs UH-Sky program for å kunne dele erfaringer fra dette arbeidet har gitt med resten av UH sektoren. En del av informasjonen som kommer frem i denne rapporten kan derfor bli delt med UH-sektoren i Norge.

Denne rapporten tar kun for seg mulige negative konsekvenser ved brudd på sikkerheten ved en utkontraktering ti Microsoft, og ikke mulighetene som dette også gir.

Dokumentreferanser

Beskrivelse	Forklaring	Peker
NTNU ROS tiltaksrapport fra ROS Office 365	NTNU Rapport med oppsummering og anbefalinger av tiltak basert på ROS rapport fra Uninett.	(Lenke til pdf her)
Forvaltningsdokument/Styrende dokument	Styrende dokument for Office 365. UH-Sky versjonen.	Lenke
Risiko- og sårbarhetsvurdering av skytjenester	Veileder fra Uninett som er lagt til grunn for arbeidet	Lenke

Gjennomføring

Risiko- og sårbarhetsvurderingen av Office 365 løsningen ble gjennomført som arbeidsmøter (workshops). Det ble gjennomført til sammen tre arbeidsmøter med deltakere fra institusjonen, Sekretariat for informasjonssikkerhet i UH-sektoren samt representanter fra UH-Sky programmet ved UNINETT. Sistnevnte deltok i stor grad som observatører.
Det første arbeidsmøte hadde fokus på deling og lagring av data gjennom Teamsites, Sharepoint og One Drive. Det andre hadde fokus på epost- og kalenderløsningen i Office 365 (Exchange Online). Det tredje og siste arbeidsmøte hadde fokus på hvilke tekniske tiltak som kan iverksettes for å redusere risikoen for de uønskede hendelsene som ble avdekket i de to første arbeidsmøtene. Man tok for seg risikoene som man hadde vurdert som særlig høye (risikoverdi 6 eller høyere). Arbeidsmøtene ble gjennomført som heldagsmøter.

Deltakerne ble tilsendt en kort forberedende informasjon til gjennomlesning før arbeidsmøtene. Disse dokumentene ligger vedlagt denne rapport.

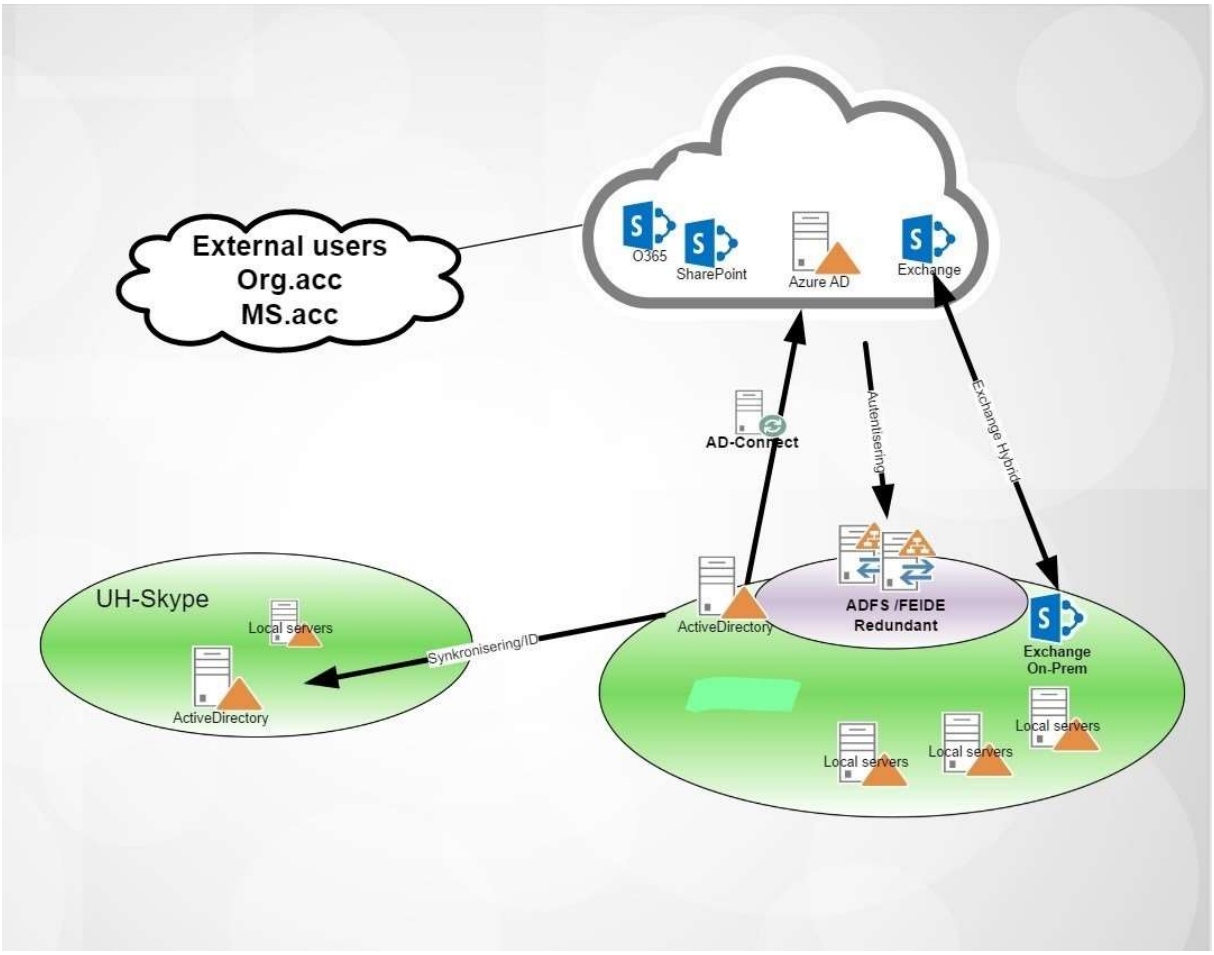
Institusjonen hadde innkalt til sammen 13 deltakere på det første arbeidsmøte (Teamsites, Sharepoint og OneDrive), 8 deltakere på det andre (Exchange online) og 12 deltakere på det siste arbeidsmøtet.

Arbeidsmøter (workshops)

Det første arbeidsmøtet hadde fokus på Sharepoint, Teamsites, og One Drive. Altså fillagring og deling i forbindelse med institusjonens bruk av løsningen.

På det andre arbeidsmøtet var fokuset rettet mot e-post og kalenderløsningen Exchange Online, og uønskede hendelser som kan hende i forbindelse med bruken av Exchange Online også for ansatte hos institusjonen. Det ble allikevel diskutert en del hendelser som ikke nødvendigvis handlet om bruken av løsningen, men mer om styring og forvaltning av løsningen.

Det tredje og siste arbeidsmøte handlet om å gjennomgå de hendelsene med høyest risiko blant hendelsene som ble diskutert i de to første arbeidsmøtene, og diskutere hvilke tekniske tiltak som kan iverksettes for å redusere risikoen til et akseptabelt nivå. På dette arbeidsmøtet deltok også en representant fra Microsoft. Rapporten vil forsøke å beskrive hvilke risikoer man står overfor ved en overgang fra dagens hybride løsning, til en løsning hvor også alle ansatte hos institusjonen benytter epost og kalender, Exchange Online, i skyen. Figuren under beskriver overordnet hvordan løsningen er satt opp i dag.


External users
Org.acc
MS.acc
O365
SharePoint
Azure AD
Exchange
AD-Connect
Autentisering
Exchange Hybrid
UH-Skype
Local servers
ActiveDirectory
Synkronisering/ID
ActiveDirectory
ADFS /FEIDE
Redundant
Exchange
On-Prem
Local servers
Local servers
Local servers

Arbeidsmøte

Arbeidsmøte ble gjennomført på følgende måte:

1. Presentasjon av deltakere.
2. Kort innføring i risikovurderingsmetodikken.
3. Felles diskusjon av hendelser som kan føre til at opplysninger som behandles i Office365 utsettes for uautorisert eksponering/tilgang, endring, sletting, tap eller utilgjengelighet.
4. Registrering av slike uønskede hendelser i regneark, se vedlagt dokument til rapporten.
5. Registrering av informasjon om hvorfor hendelsene kan oppstå (sårbarheter/svakheter) og eventuelle sikringstiltak som allerede er etablert for å redusere risikoen for hendelsene (eksisterende beskyttelses- og kontrolltiltak).
6. Felles vurdering av risikoverdien – sannsynlighet + konsekvens – for hver enkelt uønsket hendelse.
7. Verdiene for sannsynlighet og konsekvens ble vurdert med utgangspunkt i en skala fra 1 (svært lite sannsynlig/alvorlig) til 4 (svært sannsynlig/alvorlig).
8. Utarbeidelse av forslag til sikringstiltak, spesielt for uønskede hendelser med høy risiko. Dette var hendelser som deltakerne ga risikoverdien 5 eller høyere.

Punktene 3-8 er oppsummert i vedlagte regneark til rapporten.

Etter arbeidsmøtene ble regnearkene sendt ut til deltakerne for kommentarer eller justeringer. En av deltakerne hadde forslag til tiltak og kommentar etter det første arbeidsmøte. Dialogen på dette er lagt ved som billag til denne rapporten. Det var ingen andre kommentarer eller forslag til endringer.

Metodikk

Sekretariatet for informasjonssikkerhet i UH-sektoren har utarbeidet en metodikk for gjennomføring av risiko- og sårbarhetsvurderinger. Metodikken bygger på den anerkjente standarden ISO/IEC 27005:2005 («Information Security Risk Management»). Denne metodikken ble benyttet i risiko- og sårbarhetsvurderingen av Office365.

Mer utfyllende informasjon om risikovurderingsmetodikken som ble anvendt i risiko- og sårbarhetsvurderingen finnes her: https://www.uninett.no/infosikkerhet/risiko-og-s%C3%A5rbarhetsvurderinger-ros.

Risikorapport

Denne rapporten gir først en kort oppsummering av alle uønskede hendelser med risikoverdi 6 eller høyere som deltakerne avdekket og diskuterte på workshopen. Utfyllende beskrivelser av hendelsene finnes i vedlagt dokument til rapporten.

Rapporten gir dernest en mer detaljert gjennomgang av uønskede hendelser som ble vurdert å ha høy risiko, det vil si hendelser med risikoverdien 6 eller høyere. For hver av disse hendelsene spesifiseres ulike forbedringstiltak som anbefales iverksatt. Noen av disse ble foreslått og diskutert under arbeidsmøtene. Det siste arbeidsmøtet gikk i sin helhet igjennom hendelser som ble avdekket på de to første arbeidsmøtene og hadde fokus på hvilke tekniske tiltak som kunne redusere risikoen for de hendelser med risikoverdi 6 eller høyere (Rød). Det er opp til institusjonen ved risikoeier å beslutte hvilke anbefalte tiltak som eventuelt skal iverksettes.

Rapportens oppbygning

Den videre fremstillingen er delt inn i tre hoveddeler. Første del gir en oversikt over hovedfunn i risiko- og sårbarhetsvurderingen. Deretter følger en nærmere

gjennomgang over hendelser med høy risiko og anbefalte tiltak. Til slutt i del 3 gis enkelte anbefalinger med hensyn til prioritering av foreslåtte forbedringstiltak.

Del 1: Hovedfunn – oversikt

Alle hendelser

Risiko- og sårbarhetsvurderingen av Office365 ved institusjonen avdekket totalt 77 uønskede hendelser. Disse fordelte seg med 50 uønskede hendelser på arbeidsmøte med fokus på Sharepoint, Teamsites og Onedrive, og 27 uønskede hendelser fra arbeidsmøtet med fokus på epost og kalender (Exchange Online).

Dette er hendelser som kan føre til brudd på informasjonssikkerheten i opplysningene hos institusjonen.

Hendelser med høy risiko (risikoverdi 6 eller høyere)

4 av 50 uønskede hendelser ble vurdert å ha høy risiko (hendelser som deltakerne ga risikoverdi seks eller høyere) under arbeidsmøtet med fokus på Sharepoint, teamsites og OneDrive.

11 av 27 uønskede hendelser ble vurdert til å ha høy risiko under arbeidsmøtet med fokus på Exchange Online (epost/kalender).

Den høye risikoen skyldes enten at hendelsene ble vurdert som særskilt sannsynlige, at hendelsene innebar store negative konsekvenser for enkeltpersoner/institusjonen eller begge deler (både høy sannsynlighet og stor konsekvens). Se vedlagte regneark for ytterligere informasjon.

Hendelser med middels høy risiko (risikoverdi 5)

14 av 77 uønskede hendelser ble vurdert til å ha risikoverdien 5. Fem ligger i det øvre sjiktet av middels høy risiko. Vi vil anbefale at institusjonen gjør en vurdering av om man skal iverksette tiltak for alle avdekkede risikoer som har verdien 5 eller høyere.
Det anbefales at institusjonen aksepterer risikoen for de øvrige hendelsene som ble avdekket og diskutert på arbeidsmøtene, fordi risikoen for disse hendelsene ble

vurdert som lav eller relativt lav. Det innebærer at det ikke foreslås at tiltak iverksettes for å redusere sannsynligheten for eller konsekvensene av disse hendelsene. Det er imidlertid opp til institusjonen å vurdere om det likevel er ønskelig å iverksette tiltak også for enkelte av disse hendelsene.

Hovedinntrykk og overordnede risikoområder

Etter å ha gjennomført arbeidsmøtene og evaluert hendelsene observerer vi at hendelsene som ble vurdert med så vidt høy sannsynlighet og konsekvens at de kan sies å være utenfor akseptabelt risikonivå (rød, risikoverdi 6 eller høyere) dreier som om disse fire områdene:

Manglende forvaltningsregime:

Institusjonen bør etablere et godt forankret forvaltningsregime for løsningen. Mange av hendelsene peker på svakheter knyttet til ansvar og myndighetsforhold. Dette gjelder både internt hos institusjonen men også mellom institusjonen og Microsoft som databehandler. Det er også viktig at institusjonen gjør seg i stand til å forvalte sitt ansvar som behandlingsansvarlig overfor Microsoft som databehandler i henhold til gjeldende regelverk. Hendelser knyttet til manglende oppfølging av løsningen inklusive leverandør (Microsoft), ble ved flere anledninger nevnt under arbeidsmøtene.

Endringer i rammebetingelser hos Microsoft, for eksempel ved omorganiseringer/oppkjøp, økonomiske nedgangstider eller lignende må kunne håndteres av institusjonen. Dette medfører at det etableres en klar exitstrategi som gjør institusjonen i stand til å skifte ut leverandør uten at dette skaper kritiske situasjoner.

Menneskelig feil av bruker:

Løsningen vil medføre at brukerne kan dele informasjon med andre. Enten dette er eksterne brukere eller interne brukere. Flere av hendelsene går ut på at brukeren gjør feil ved deling av dokumenter, eller feil ved deling av tilganger. Man kan også glemme å ta bort tilganger som tidligere er gitt. Ved en skyløsning som Office365

kan brukerne selv sette opp tilganger til dokumenter eller mapper. Dette innebærer at brukerne må være årvåkne både ved tildeling av rettigheter og å sjekke hvem som har tilgang til dokumentene.

Brukere kan også feilaktig laste opp dokumenter i skyen som ikke egner seg til å legge ut i skyen. Det kan også være brudd på regulatoriske eller avtalemessige forhold. Oppdragsforskning med spesielle krav til beskyttelse kan være eksempel på slik informasjon. Mange av hendelsene som kom frem handlet om disse forhold.

Brukernavn og passord på avveier er en hendelse som kan få store konsekvenser i en slik løsning. Dersom man har en konto som er på avveier vil man kunne oppleve at en ondsinnet aktør kan ha lagt inn egne tilganger eller delt områder som senere kan utnyttes selv om eieren av brukerkontoen skifter passord.

Bærbare eller håndholdte enheter:

Det benyttes stadig mer bærbare eller håndholdte enheter til behandling av informasjon. Smart-telefoner eller nettbrett med internettilgang er typiske eksempler som de fleste har tilgang på. Institusjonen har manglende styring av håndholdte enheter og hvorvidt de er sikret med pinkode eller passord med tilsvarende styrke som man krever i systemløsningene som er tilgjengelig via denne. Det er ofte slik at dersom man først får åpnet en håndholdt enhet, har man direkte tilgang til de applikasjoner som ligger i denne, ofte uten å måtte skrive passord pånytt. Dersom en håndholdt enhet blir mistet eller stjålet, er det derfor stor sannsynlighet for og konsekvens ved at denne blir utnyttet.

Sikkerhetskopiering:

Løsningen til Microsoft inneholder ikke en reell sikkerhetskopiering. Men på grunn av redundans og robusthet innebygget i løsningen, har man mulighet til å få tilbake data som er opptil 90 dager gamle. Institusjonen vurderte dette som en stor risiko, og her må man også vurdere muligheten for evig tap av data.

Avhengighet til Microsoft:

Institusjonen har allerede med dagens løsning erfart at det tar mye lengre tid å rette opp kritiske feil i systemet. For eksempel dersom man oppdager en «phising» angrep som kan skade institusjonen, vil dette kunne ta uakseptabel lang tid å få rettet på via Microsoft. Her er det stor forskjell på lokal løsning og sky-løsning. Det å ikke kunne respondere raskt nok på hendelser fordi man er avhengig av kapasiteten til en ekstern aktør er vurdert til å ha en høy risiko.

Et annet forhold som ble diskutert er at man er avhengige av å kjøre løsningen slik Microsoft har bestemt. Dette medfører at det kan være vanskelig å etablere egne nødvendige sikkerhetstiltak eller sikkerhetsarkitektur, fordi dette ikke er en del av Microsoft sitt tilbud.

Manglende brukeropplæring:

Mange av hendelsene som ble diskutert på arbeidsmøtene skyldtes at brukerne mangler kompetanse eller informasjon om løsningen. Hvor lagres dataene? hvordan sikrer jeg at jeg deler de riktige dokumentene/mappene med riktige brukere?, og hva kan man faktisk bruke Office365 løsningen til?

Det kom også frem uønskede hendelser som skyldes manglende kompetanse fra de som jobber på IT-drift.

Det foreslås at det iverksettes forbedringstiltak innenfor følgende tiltakskategorier:

1. God forvaltning av tjenesten
2. Opplæring til brukere, inkludert driftspersonell
3. Etablering av rutiner og retningslinjer.
4. Tekniske forbedringstiltak.

Nedenfor følger en gjennomgang av alle hendelser med høy eller relativt høy risiko. Det foreslås forbedringstiltak for hver av disse hendelsene.

Del 2: Hendelser med høy risiko og anbefalte tiltak – fokus på Sharepoint, teamsites og OneDrive

Risikoelement/hendelse 16	Sårbarhet	Eksisterende tiltak	S	K	Risiko
Uvedkommende får tilgang til sensitive data	Deling av brukernavn/passord på grunn av holdninger eller mangelfull kompetanse/bevissthet	Passordpolicy	4	3	7
Tiltak	**Tiltakskategori: Teknisk og administrativt**				
Innføre policy som ikke tillater en bruker å gi en gruppe tilgang til sensitive data (sensitive personopplysninger, forskningsdata med særskilt behov for beskyttelse eller virksomhetskritisk informasjon). 2. faktor autentisering. Aktivere og lage et konsept for IRM (Information Rights Management). Opplæring i hvordan man setter opp og konfigurerer IRM er avgjørende for resultatet. Basert på innhold kan man veilede brukeren ved lagring/sending. Sørge for tilstrekkelig kompetanseheving for de som skal drifte løsningen. Det må etableres et forvaltningsregime, ansvar roller og kompetanse. Etableres et internt apparat for gjennomgang av logger/oppfølging Redusere antall med global admin til et minimum					

Risikoelement/hendelse 9	Sårbarhet	Eksisterende tiltak	S	K	Risiko
Mangelfull sikring av forskningsdata, konfidensialitet	Sensitive forskningsdata lagres i O365 pga manglende informasjon til brukermiljøet om retningslinjer for hvor ulike type data skal eller kan lagres	Generell informasjon via banner på O365 åpningsside og info om sikkerhet nederst på siden	3	3	6
Tiltak	**Tiltakskategori: Teknisk og administrativt**				

Innføre policy som ikke tillater en bruker å gi en gruppe tilgang til sensitive data (sensitive personopplysninger, forskningsdata med særskilt behov for beskyttelse eller virksomhetskritisk informasjon).

2. faktor autentisering.

Aktivere og lage et konsept for IRM (Information Rights Management). Opplæring i denne sammenheng er viktig.

Basert på innhold kan man veilede brukeren ved lagring/sending.
Sørge for tilstrekkelig kompetanseheving for de som skal drifte løsningen.

Det må etableres et forvaltningsregime, ansvar roller og kompetanse.

Etableres et internt apparat for gjennomgang av logger/oppfølging
Det må vurderes hva som skal aktiveres basert på lover og regler.

Risikoelement/hendelse 14	Sårbarhet	Eksisterende tiltak	S	K	Risiko
Sensitive data på avveie	Mangelfull sikkerhet på håndholdt/bærbart IT-utstyr pga. lagring av passord på enheten. Dermed er det bare eventuell skjermlås som hindrer uvedkommende å få tilgang til data som ellers er underlagt passordpolicy. (smarttelefoner/nettbrett). Kan lett mistes eller bli stjålet.	Passordpolicy	3	3	6
Tiltak	**Tiltakskategori: Teknisk og administrativt**				
IRM eller ADFS kan begrense mulighet for tilgang til dokumenter med en spesiell klassifisering. Vurdere å tilgjengeliggjøre E5 lisens for enkeltmiljøer med særskilt behov for beskyttelse. Skru på customer lock box (E5) Klassifisering av informasjon er en forutsetning her.					

Risikoelement/hendelse 26	Sårbarhet	Eksisterende tiltak	S	K	Risiko
Data er utilgjengelig	Manglende historiske back-up, data slettes etter 90 dager		3	3	6
Tiltak	**Tiltakskategori: Teknisk og administrativt**				
Implementere en 3. parts backupløsning som inngår i forvaltningsregime.					

Del 2: Hendelser med høy risiko og anbefalte tiltak - fokus på Exchange Online

Risikoelement/hendelse 11	Sårbarhet	Eksisterende tiltak	S	K	Risiko
Lavere kvalitet på tjenesten. Nedetid. Tap av tillit til tjenesten. Kostnader for ekstra driftstjenester. Tap av kontroll.	Større avstand til driftsmiljøet. Hendelser kan ikke løses lokalt. Det tar lengre til å rette opp feil. Manglende eller dårlig logging av hendelser. Man blir varslet om hendelser som ikke nødvendigvis rammer institusjonen. Man har allerede høstet erfaring på at det kan ta lang tid å få gjennomført tiltak etter hendelser.		4	4	8
Tiltak	**Tiltakskategori: Teknisk og administrativt**				
Microsoft må jobbe med å få bedre filtrering på varslene. Premier support avtale skal være til hjelp. Etablere gode rutiner for hva som skjer ved brudd på SLA/avtaler. Benytte «security and compliance center» for å få informasjon ved avvik.					

Risikoelement/hendelse 29	Sårbarhet	Eksisterende tiltak	S	K	Risiko
Begrenset funksjonalitet og tilgang. Angrep pågår lengre.	Lav hastighet på kommunikasjonslinjer, båndbredde, latency. Man får også begrensninger i for hold til drift av løsningen. "Verktøy går tregere." Respons på hendelser tar lengre tid. Fra under en time til flere dager.gjennomført tiltak etter hendelser.		4	4	8
Tiltak	**Tiltakskategori: Teknisk og administrativt**				
Sette ut en management maskin i Azure slik at script for fjerning av f.eks. phising går raskere. Sørge for å kunne kommunisere med Microsoft om egne funn av phising eposter slik at Microsoft på sin side kan fjerne eller edusere konsekvensen av angrepet. Vurdere E5 (lisens med utvidet funksjonalitet), «advanced threat protection vil stoppe flere angrep.»					

Risikoelement/hendelse 8	Sårbarhet	Eksisterende tiltak	S	K	Risiko
Brudd på informasjons konfidensialitet, integritet eller tilgjengelighet. Tap av tillit til tjenesten.	O365 er et større mål enn institusjonens eksisterende løsning. Man kan få en større eksponering for angrep.		4	4	8
Tiltak	**Tiltakskategori: Teknisk og administrativt**				
Vurdere E5 (lisens med utvidet funksjonalitet), «advanced threat protection vil stoppe flere angrep.» Vaske mailen lokalt hos institusjonen eller i UH sektoren					

Risikoelement/hendelse 9	Sårbarhet	Eksisterende tiltak	S	K	Risiko
Brudd på informasjons konfidensialitet, integritet eller tilgjengelighet. Tap av tillit til tjenesten.	Det er lett for en trusselaktør å kartlegge sikkerhetsløsningen på grunn av at den er "Microsoft standard". Større fare for angrep/sikringsbrudd.		3	4	7
Tiltak	**Tiltakskategori: Teknisk og administrativt**				
Sette ut en management maskin i Azure slik at script for fjerning av f.eks. phising går raskere. Sørge for å kunne kommunisere med Microsoft om egne funn av phising eposter slik at Microsoft på sin side kan fjerne eller redusere konsekvensen av angrepet. Vurdere E5, «advanced threat protection vil stoppe flere angrep.» Kryptere egne mailbokser vha E5 Rydde i Exchangeadmin på Exchange Online					

Risikoelement/hendelse 12	Sårbarhet	Eksisterende tiltak	S	K	Risiko
Brudd på norsk lovverk. Brudd på informasjons konfidensialitet, integritet eller tilgjengelighet. Tap av tillit til tjenesten.	Manglende oversikt over norsk lovverk, og hvordan en utsetting i skyen påvirker dette. Man har ikke gjort en kartlegging av hva eposter inneholder, og dermed ikke vet hva slags informasjon som flyttes ut til skyen.		4	3	7
Tiltak	**Tiltakskategori: Teknisk og administrativt**				
Retningslinjer, rutiner og holdningsskapende arbeid. Dette bør avklares med juridisk personell hos institusjonen.					

Risikoelement/hendelse 19	Sårbarhet	Eksisterende tiltak	S	K	Risiko
Brudd på norsk lovverk. Brudd på informasjons konfidensialitet. Tap av tillit til tjenesten. Økonomisk tap.	Man lagrer informasjon i skyen som etter norsk lov skal beskyttes spesielt. F.eks. personopplysninger og helseopplysninger.		4	3	7
Tiltak	**Tiltakskategori: Teknisk og administrativt**				
Retningslinjer, rutiner og holdningsskapende arbeid. - Dette bør avklares med juridisk personell hos institusjonen.					

Risikoelement/hendelse 10	Sårbarhet	Eksisterende tiltak	S	K	Risiko
Brudd på informasjons konfidensialitet, integritet eller tilgjengelighet. Tap av tillit til tjenesten.	Man mister muligheten for å selv utvikle sin egen sikkerhetsløsning, mister helhetsbildet og oversikt over trusselaktører og angrepsvektorer. Man er avhengig av Microsofts standardløsninger. Microsoft sitter ikke på lokal kompetanse om institusjonens behov. Fare for at epost som skal mottas stoppes av Microsofts contentfilter.		2	4	6
Tiltak	**Tiltakskategori: Teknisk og administrativt**				
Sørge for tilgang til logger fra Microsoft. Vasking av egen epost, for å stoppe eventuelle skadevare i en epost.					

Risikoelement/hendelse 16	Sårbarhet	Eksisterende tiltak	S	K	Risiko
Brudd på norsk lovverk. Brudd på informasjons konfidensialitet, integritet eller tilgjengelighet. Tap av tillit til tjenesten.	Manglende tilpassing av egen arkitektur. Den må understøtte bruk av sky-tjenester. Det er en fare for at man ikke får tilstrekkelig med økonomiske rammevilkår for å etablere en god løsning.	IT-avtalene er samlet i en gruppe. Dette gir muligheter for bedre porteføljestyring og oversikt.	3	3	6
Tiltak	**Tiltakskategori: Teknisk og administrativt**				
Sørge for god lederforankring tidlig i prosjektet slik at man kan gjøre god planlegging, testing og sikre seg tilstrekkelige rammevilkår for en god løsning.					

Risikoelement/hendelse 23	Sårbarhet	Eksisterende tiltak	S	K	Risiko
Brudd på norsk lovverk. Brudd på informasjons konfidensialitet, integritet eller tilgjengelighet. Tap av tillit til tjenesten. Økonomisk tap.	Uklart dataeierskap internt kan gi dårlig dataforvaltning og manglende retningslinjer. Hendelser kan få større konsekvens ved lagring i skyen.		3	3	6
Tiltak	**Tiltakskategori: Teknisk og administrativt**				
Iverksette et godt forvaltningsregime. Det er laget et eget styrende dokument for forvaltning. Dette dokumentet må utvides til også å inneholde hvordan institusjonen skal ivareta sitt ansvar som behandlingsansvarlig. Dokumentet må følges opp og iverksettes.					

Risikoelement/hendelse 5	Sårbarhet	Eksisterende tiltak	S	K	Risiko
Tap av informasjon. Tap av tillit til tjenesten. Økonomisk tap.	Prosjektet gjør forutsetninger som ikke kommuniseres ut til brukere i tilstrekkelig grad. Eller at kommunikasjonen til brukerne er vanskelig å forstå.		4	2	6
Tiltak	**Tiltakskategori: Teknisk og administrativt**				
Risikovurdering i prosjektet. God kartlegging, for eksempel sørge for at brukerne forstår hvordan sikkerhetskopiering foregår. Se for øvrig risikoelement nr. 12.					

Risikoelement/hendelse 20	Sårbarhet	Eksisterende tiltak	S	K	Risiko
Man følger ikke opp sitt ansvar som behandlingsansvarlig. Brudd på norsk lovverk. Brudd på informasjons konfidensialitet, integritet eller tilgjengelighet. Tap av tillit til tjenesten. Økonomisk tap.	Det er vanskelig å få revidert en så stor leverandør som Microsoft, eller en unnlater å følge opp sitt ansvar som behandlingsansvarlig.		4	2	6
Tiltak	**Tiltakskategori: Teknisk og administrativt**				
Institusjonen etablerer et regime for kontroll med og oppfølging av Office365. Dette innebærer at det utpekes en person hos institusjonen som er ansvarlig for å etterspørre og gjennomgå dokumentasjon fra Microsoft som viser hvordan vilkår i avtaler for løsningen etterleves av Microsoft. Slik dokumentasjon kan for eksempel være rapporter fra sikkerhetsrevisjoner og risiko- og sårbarhetsvurderinger som Microsoft har gjennomført. Eventuelle avvik fra avtalevilkår skal formidles til Microsoft og det skal kreves at avvikene lukkes.					

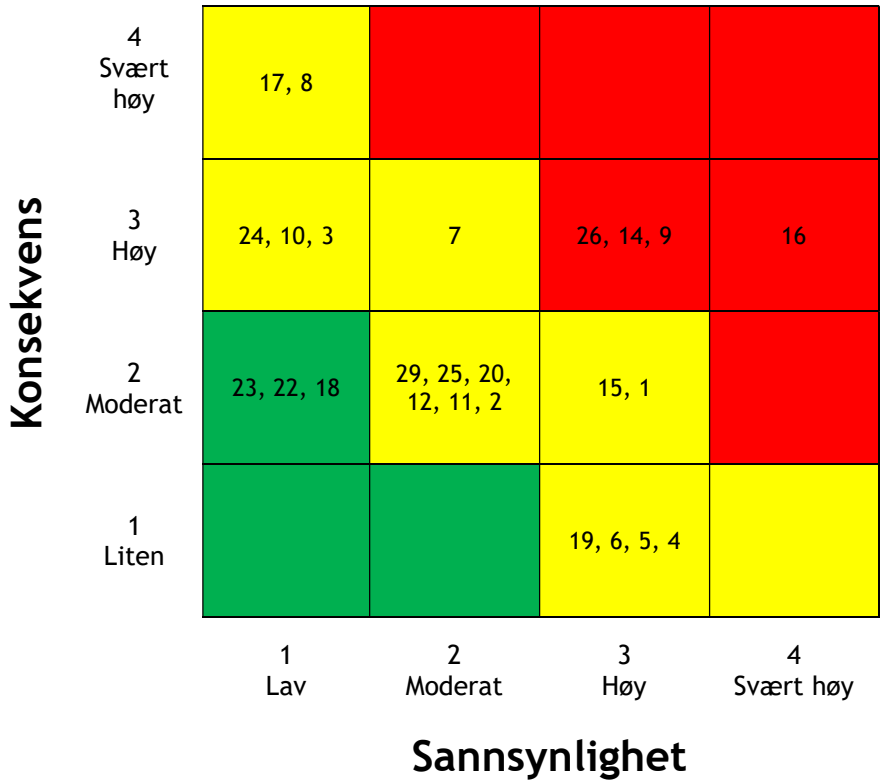
Del 3: Tiltaksprioritering

1) Institusjonen bør etablere et forvaltningsregime som er forankret i toppledelsen for Office365 løsningen. Mange av hendelsene peker på svakheter knyttet til ansvar og myndighetsforhold og etablering av rutiner og retningslinjer.
2) Skaffe seg oversikt over informasjonsverdier og innføre en klassifisering av informasjon.
3) Etablere rutiner for sikkerhetsopplæring, holdningskampanjer for å skape en god sikkerhetskultur.
4) Etablere et regime for å styre bærbare eller håndholdte enheter, eller sørge for at slike ikke reduserer den sikkerheten som vanlige klienter er underlagt.
5) Vurdere behov for backup av data i løsningen gjennom 3. partsverktøy
6) Redusere avhengigheten til en leverandør, i dette tilfellet Microsoft ved å lage en strategi for hvordan man går ut av, eller endrer leverandør. Her vil også kontinuitetsplaner være viktige.
7) Institusjonen bør sørge for å gi brukerne tilstrekkelig opplæring for å minimalisere sannsynligheten for at de vil gjøre feil.
8) Etablere tekniske løsninger som tilbys for å kryptere informasjon og hindre utilsiktede feil.

Generelt sett bør institusjonen som minimum vurdere å etablere tiltak for alle hendelser med risikoverdi 6 eller høyere. Det er også viktig at hendelser med lavere risikoverdi enn 6 blir vurdert, enten med å etablere tiltak, eller at ansvarlige aksepterer denne risikoen.

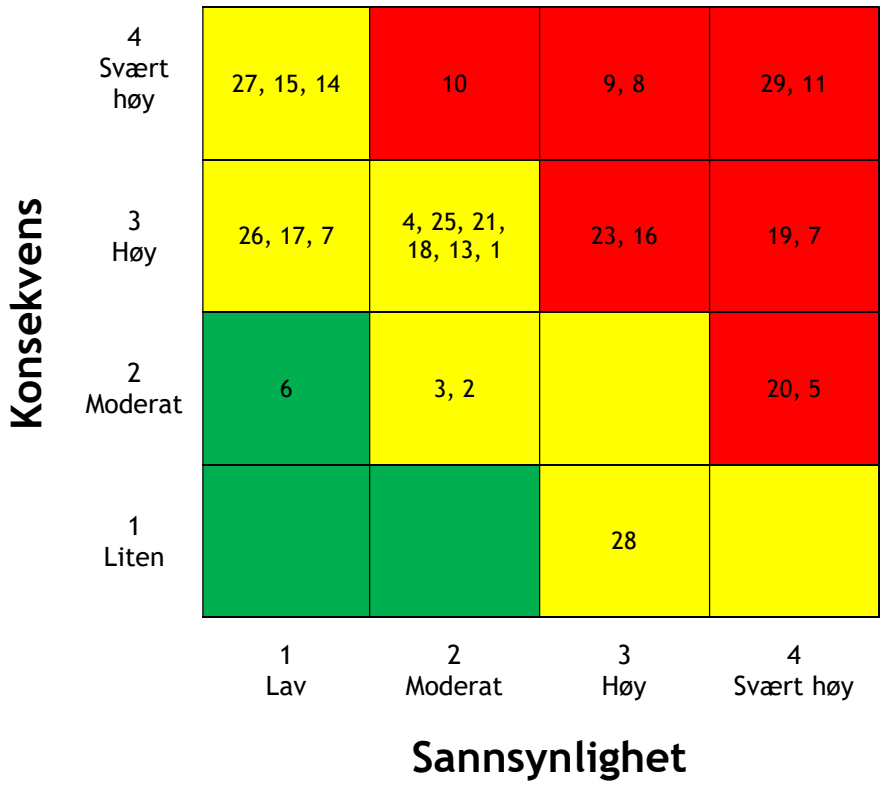
Vedlegg 1: Risikomatrise – Arbeidsmøte 1, Sharpoint, teamsites og OneDrive

Hver av hendelsene som ble identifisert på arbeidsmøtet er nummerert og puttet inn i risikomatrisen under.



Vedlegg 2: Risikomatrise – Arbeidsmøte 2, Exchange Online

Hver av hendelsene som ble identifisert på arbeidsmøtet er nummerert og puttet inn i risikomatrisen under.



Vedlegg 3: Utklipp av utfylt regneark til denne rapporten

1. arbeidsmøte

NB Unntatt offentligheten.

Vedlegg 4: Melding til deltakerne i risiko- og sårbarhetsvurderingen – 1. arbeidsmøte

Melding til deltakere i risikovurdering

Velkommen til arbeidsmøte for risikovurdering av Office365 ved institusjonen.
Arbeidsmøtet vil fokusere på risikoforhold knyttet til elektronisk behandling av data, spesielt personopplysninger, som registreres i og behandles av skytjenesten Office365.
Som forberedelse til arbeidsmøtet, ønsker vi at du tar noen minutter til å lese igjennom dette dokumentet.

Risikovurderinger

Risikovurdering spiller en sentral rolle i arbeidet med å sikre at institusjonen behandler data, spesielt personopplysninger, på en trygg og sikker måte.
Risikovurderinger kan virke som noe fremmed og teknisk. Det er det ikke. Vi gjør alle risikovurderinger hver eneste dag. Vi vurderer for eksempel risikoen for trafikkulykker som så liten at vi kjører bilen til jobben hver morgen. Vi aksepterer denne risikoen. Men vi forlater ikke bilen ulåst på parkeringsplassen utenfor kjøpesenteret. Denne risikoen aksepterer vi ikke.
Hvis vi tar utgangspunkt i det siste eksempelet, kan vi si at risikovurderinger består av en beskrivelse av hva som skal risikovurderes:
"Bilen står ulåst på parkeringsplassen utenfor kjøpesenteret."
Så spør vi: hvilke uønskede hendelser kan skje?

- Bilen kan bli stjålet.

- Noe i bilen kan bli stjålet, for eksempel stereoanlegget eller fotoapparatet.

Til slutt vurderer vi hvor sannsynlig det er at disse to uønskede hendelsene inntreffer og hvilke negative konsekvenser det i så fall kan få for oss.
Dersom vi da finner ut at sannsynligheten for og konsekvensene av hendelsene er stor, vil risikoen være uakseptabel høy. Løsningen blir da å iverksette ulike typer sikringstiltak, for eksempel å låse bilen, utstyre den med alarm, osv.
Det er denne typen vurderinger du er invitert til å delta på når det gjelder Office365.
Spørsmålene som vil bli drøftet på arbeidsmøtet er risikoen for:

- Brudd på konfidensialiteten – uvedkommende får tilgang til data/personopplysninger

- Brudd på integriteten – uvedkommende endrer, redigerer eller sletter data/personopplysninger.

- Brudd på tilgjengeligheten – rette vedkommende får ikke tilgang til data/personopplysninger når han/hun har behov for det.

Arbeidsmøtets formål er derfor å (1) identifisere hvilke data, spesielt personopplysninger, som registreres i og behandles i Office365, (2) identifisere tenkbare uønskede hendelser som kan oppstå i forbindelse med Office365 og (3) vurdere hendelsenes sannsynlighet og konsekvens.

Tenk igjennom

Tenk igjennom hvilke uønskede hendelser som kan oppstå i forbindelse med bruken av de ulike produktene i Office365. Er det noe som kan føre til uautorisert tilgang, endring, skade eller tap av data/personopplysninger?
Nedenfor finner du noen eksempler på uønskede hendelser.
Tenk igjennom om du har opplevd eller kan komme på andre typer uønskede hendelser som kan oppstå i forbindelse med bruken av de nevnte IT-systemene.
Eksempler på uønskede hendelser

- Brudd på konfidensialiteten til personopplysninger, eller andre opplysninger med behov for beskyttelse som er registrert i systemet fordi uvedkommende har fått tilgang til brukernavn/passord.

- Brudd på integriteten til personopplysninger fordi uvedkommende utnytter tilgangen til å endre opplysninger om utvalgte personer eller annen informasjon slik at de blir feilaktige.

- Brudd på tilgjengeligheten til personopplysningene fordi systemet utsettes for hackerangrep eller tjenestenektangrep.

Vedlegg 5: Melding til deltakerne i risiko- og sårbarhetsvurderingen – 2. arbeidsmøte

Melding til deltakere i risikovurdering

Velkommen til arbeidsmøte for risikovurdering av Office365 ved institusjonen.
Arbeidsmøtet vil fokusere på risikoforhold knyttet til elektronisk behandling av data, spesielt personopplysninger, som registreres i og behandles ved epost og kalendertjenester som ligger under Exchange.
Som forberedelse til arbeidsmøtet, ønsker vi at du tar noen minutter til å lese igjennom dette dokumentet.

Risikovurderinger

Risikovurdering spiller en sentral rolle i arbeidet med å sikre at institusjonen behandler data, spesielt personopplysninger, på en trygg og sikker måte.
Risikovurderinger kan virke som noe fremmed og teknisk. Det er det ikke. Vi gjør alle risikovurderinger hver eneste dag. Vi vurderer for eksempel risikoen for trafikkulykker som så liten at vi kjører bilen til jobben hver morgen. Vi aksepterer denne risikoen. Men vi forlater ikke bilen ulåst på parkeringsplassen utenfor kjøpesenteret. Denne risikoen aksepterer vi ikke.
Hvis vi tar utgangspunkt i det siste eksempelet, kan vi si at risikovurderinger består av en beskrivelse av hva som skal risikovurderes:
"Bilen står ulåst på parkeringsplassen utenfor kjøpesenteret."
Så spør vi: hvilke uønskede hendelser kan skje?

- Bilen kan bli stjålet.
- Noe i bilen kan bli stjålet, for eksempel stereoanlegget eller fotoapparatet.

Til slutt vurderer vi hvor sannsynlig det er at disse to uønskede hendelsene inntreffer og hvilke negative konsekvenser det i så fall kan få for oss.
Dersom vi da finner ut at sannsynligheten for og konsekvensene av hendelsene er stor, vil risikoen være uakseptabel høy. Løsningen blir da å iverksette ulike typer sikringstiltak, for eksempel å låse bilen, utstyre den med alarm, osv.
Det er denne typen vurderinger du er invitert til å delta på når det gjelder Office365.
Spørsmålene som vil bli drøftet på arbeidsmøtet er risikoen for:

- Brudd på konfidensialiteten – uvedkommende får tilgang til data/personopplysninger
- Brudd på integriteten – uvedkommende endrer, redigerer eller sletter data/personopplysninger.
- Brudd på tilgjengeligheten – rette vedkommende får ikke tilgang til data/personopplysninger når han/hun har behov for det.

Arbeidsmøtets formål er derfor å (1) identifisere hvilke data, spesielt personopplysninger, som registreres i og behandles i Office365, (2) identifisere tenkbare uønskede hendelser som kan oppstå i forbindelse med Office365 og (3) vurdere hendelsenes sannsynlighet og konsekvens.

Tenk igjennom

Tenk igjennom hvilke uønskede hendelser som kan oppstå i forbindelse med bruken av epost og kalendertjenester. Er det noe som kan føre til uautorisert tilgang, endring, skade eller tap av data/personopplysninger?
Nedenfor finner du noen eksempler på uønskede hendelser.
Tenk igjennom om du har opplevd eller kan komme på andre typer uønskede hendelser som kan oppstå i forbindelse med bruken av de nevnte IT-systemene.
Eksempler på uønskede hendelser

- Brudd på integritet, tilgjengelighet og konfidensialitet til personopplysninger, eller andre opplysninger med behov for beskyttelse fordi uvedkommende har fått tilgang til brukernavn/passord, og kan opptre på vegne av deg.

- Brudd på konfidensialiteten til personopplysninger fordi epost med sensitiv informasjon går til feil mottaker eller gruppemottakere.

- Brudd på tilgjengeligheten fordi skyleverandøren har et massivt DDOS angrep rettet mot seg.

Brudd på tilgjengeligheten fordi tilgang til internett er nede