|  |
| --- |
| Rapporttittel: Risiko- og sårbarhetsvurdering av Office 365, Sharepoint, teamsites, fillaggring/deling/samarbeid ved NTNU  Forfatter: Rolf Sture Normann  Dato: 21.06.2016  Rapporten er unntatt offentlighet i henhold til Offentleglova § 13 og Forvaltningsloven § 13. |

Innhold

[Forord 3](#_Toc454363315)

[Oppsummering 4](#_Toc454363316)

[Følgende hovedtyper tiltak anbefales iverksatt: 4](#_Toc454363317)

[Innledning 5](#_Toc454363318)

[Dato og gjennomføring 5](#_Toc454363319)

[Systemprofil 6](#_Toc454363320)

[Resultat fra risiko- og sårbarhetsvurderingen 7](#_Toc454363321)

[Risikonivå 7](#_Toc454363322)

[Anbefalte tiltak 8](#_Toc454363323)

[Vedlegg A Kopi av ROS-regneark 11](#_Toc454363324)

[Kommentarer fra deltakerne 13](#_Toc454363325)

# Forord

Sekretariat for informasjonssikkerhet i UH sektoren er opprettet av Kunnskapsdepartementet og lagt til UNINETT AS.

Formålet med sekretariatet er å bidra til at UH-sektoren oppnår tilfredsstillende informasjonssikkerhet. Nasjonal strategi for informasjonssikkerhet skal ligge til grunn for sekretariatets arbeid. <https://www.regjeringen.no/globalassets/upload/fad/vedlegg/ikt-politikk/nasjonal_strategi_infosikkerhet.pdf>

Sekretariatet har utarbeidet en metodikk for gjennomføring av risiko- og sårbarhetsvurderinger, som bygger på den anerkjente standarden ISO/IEC 27005:2005 («Information Security Risk Management»). Denne metodikken er benyttet i risiko- og sårbarhetsvurderingen av LMS.

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

# Oppsummering

Risiko- og sårbarhetsvurderingen av Office365 Sharepoint/teamsite/fil/lagring og deling avdekket 29 hendelser som kunne føre til brudd på informasjonssikkerheten.

For 4 av hendelsene ble risikoen vurdert som såpass alvorlig/kritisk (høy risiko) at det er nødvendig med iverksetting av forbedringstiltak. Dette for å unngå at hendelsene påvirker informasjonssikkerheten i systemet på en negativ måte.

For 18 av hendelsene ble risikoen vurdert som middels høy. Dette innebærer at virksomheten også her bør vurdere å iverksette tiltak (Gul).

For 3 av hendelsene ble risikoen vurdert som så liten at tiltak ikke er nødvendig.

For 4 av hendelsene var vi ikke i stand til å vurdere sannsynlighet på grunn av usikkerhet knyttet til den aktuelle hendelsen. Usikkerhetsfaktorene bør sjekkes ut slik at man er oppmerksomme på problemstillingen hendelsen reiser.

## Følgende hovedtyper tiltak anbefales iverksatt:

* Administrativt
  + Tilstrekkelig opplæring av brukere
  + Kultur og holdningsskapende kampanjer, opplysningskampanjer
  + Etablering av rutiner og policy ved bruk
* Teknisk
  + Etablere rollestyrte tilganger
  + Innføre Mobile Device Management (MDM), dette medfører sentral styring av smarttelefoner og nettbrett
  + Benytte ePhorte i større grad for arkivverdig informasjon

Hendelsene og tilhørende tiltak er nærmere beskrevet under punktet «Anbefalte tiltak». Tiltakene er beskrevet på et overordnet nivå. NTNU må selv vurdere og ta nærmere stilling til hvordan de skal utformes og iverksettes slik at man oppnår tilfredsstillende informasjonssikkerhet.

# Innledning

## Dato og gjennomføring

ROS-workshopen ble holdt 24. mai 2016 på NTNU, Gløshaugen. Deltakerne var fra NTNU med observatører frå UNINETT UH\_Sky programmet. ROSen ble fasilitert av UH-sektorens sekretariat for informasjonssikkerhet hos UNINETT.

På grunn av at man i ROS-rapporten beskriver sensitive forhold vedrørende bruken av Office365, kan deler av rapporten unntas offentlighet i henhold til Offentleglova § 13 og Forvaltningsloven § 13. Det anbefales at man vurderer om det er forhold i rapporten som omtaler enheter/avdelinger på en slik måte at det kan skade infomasjonssikkerheten om den skulle komme på avveie.

Rapporten er utarbeidet av Rolf Sture Normann og Tommy Tranvik ved UH-sektorens sekretariat for informasjonssikkerhet med innspill fra deltakerne.

Deltakere

|  |  |  |
| --- | --- | --- |
| Navn | Rolle | Institusjon |
| Ole Langfeldt |  | NTNU |
| Snorre Jenssen |  | NTNU |
| Rolf Sture Normann | Sekretariat for informasjonssikkerhet i UH sektoren | UNINETT |
| Tommy Tranvik | Sekretariat for informasjonssikkerhet i UH sektoren | UNINETT |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Systemprofil

|  |  |
| --- | --- |
| **Tjeneste/System** | LMS |
| **Risikoeier** |  |
| **Virksomhetsområde** |  |
| **Utbredelse** |  |
| **Beskrivelse** | Office365 Sharepoint/Teamsite lagring og deling av dokumenter |
| **Leverandør** | Microsoft |
| **Driftes av** | Microsoft |

# Resultat fra risiko- og sårbarhetsvurderingen

## Risikonivå

Det ble i ROSen identifisert 29 risikoelementer (uønskede hendelser). Fordelingen mellom risikonivåene er vist i tabellen under.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Risikonivå | Høy | Medium | Lav | Udefinert |
| Antall | 4 | 18 | 3 | 4 |

Risikoelementet med lav risiko (grønn) vil ikke vurderes spesielt i denne rapporten men tas med slik at de evt. kan vurderes på nytt ved senere risiko- og sårbarhetsvurderinger.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Risikoelementene er for oversiktens skyld markert i matrisen under.   |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | **Konsekvens** | 4  Svært  høy | 8, 17 |  |  |  | | 3  Høy | 3, 10, 24 | 7 | 9,14,26 | 16 | | 2  Moderat | 18, 22, 23 | 2, 11, 12, 20, 25, 29 | 5, 15 |  | | 1  Liten |  |  | 4, 5, 6, 19 |  | |  | 1  Lav | 2  Moderat | 3  Høy | 4  Svært høy | |  | **Sannsynlighet** | | | | | |  |  |

## Anbefalte tiltak

Tiltakene som er presentert i tabellene ble identifisert under workshopen. Det er risikoeiernes ansvar å eventuelt komme med ytterligere tiltak eller endre de foreslåtte tiltakene.

Tiltakskortene baserer seg på uønskede hendelser som ble vurdert med risikofaktor 5 eller høyere. Dette medfører alle høyere middels, (Gul) og alle med høy risikoverdi (rød).

|  |  |  |  |
| --- | --- | --- | --- |
| **Tiltakskort nr. 1** | |  |  |
| Organisasjon: | NTNU | Risiko | Tiltak |
| Tiltakstype: | Administrativt | Uvedkommende får tilgang til sensitive data  Deling av brukernavn/passord på grunn av holdninger eller mangelfull kompetanse/bevissthet | Gjentagende påminnelser til brukere. |
| Risikoelement: | **16** |
| Risikonivå: | **Høy** |
| Anm: Det er laget passordpolicy ved NTNU | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Tiltakskort nr. 2** | |  |  |
| Organisasjon: | NTNU | Risiko | Tiltak |
| Tiltakstype: | Administrativt | 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. | IRM, policy for behandling av forskningsdata, info til forskere |
| Risikoelement: | **9** |
| Risikonivå: | **Høy** |
| Anm: Informasjon via banner på O365 åpningsside og informasjon om sikkerhet nederst på denne siden. | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Tiltakskort nr. 3** | |  |  |
| Organisasjon: | NTNU | Risiko | Tiltak |
| Tiltakstype: | Teknisk | 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. | Innføre MDM, Mobile Device Management. Sentral styring av smarttelefoner/nettbrett. |
| Risikoelement: | **14** |
| Risikonivå: | **Høy** |
| Anm: Det er laget passordpolicy ved NTNU | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Tiltakskort nr. 4** | |  |  |
| Organisasjon: | NTNU | Risiko | Tiltak |
| Tiltakstype: | Administrativt | Data er utilgjengelig  Manglende historiske back-up, data slettes etter 90 dager | Data av juridisk eller forvaltningsmessig verdi må over i ePhorte (jf NTNUs arkivplan og regler for bevaring/kassasjon). |
| Risikoelement: | **26** |
| Risikonivå: | **Høy** |
| Anm: | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Tiltakskort nr. 5** | |  |  |
| Organisasjon: | NTNU | Risiko | Tiltak |
| Tiltakstype: | Administrativt | Sensitive dokumenter eller opplysninger deles med feil person eller feil gruppe. Kan også føre til uautorisert endring/sletting.  Brukerfeil - Uriktig bruk av "share with everyone"-mappen på grunn av manglende kompetanse om hvordan denne delingsmuligheten fungerer. | Brukeropplæring og informasjon |
| Risikoelement: | **1** |
| Risikonivå: | **Middels** |
| Anm: | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Tiltakskort nr. 6** | |  |  |
| Organisasjon: | NTNU | Risiko | Tiltak |
| Tiltakstype: | Administrativt | Uautorisert tilgang til sensitive data etter at tilgangen skulle vært avsluttet, kan misbrukes  Brukertilganger til dokumenter eller data endres ikke når personer endrer rolle/stilling internt eller slutter. Dermed blir tilganger til data man ikke skal ha tilgang til liggende igjen. | Innføre rollestyrt tilgang |
| Risikoelement: | **7** |
| Risikonivå: | **Middels** |
| Anm: Satt i gang tiltak for automatisk sletting av brukere | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Tiltakskort nr. 7** | |  |  |
| Organisasjon: | NTNU | Risiko | Tiltak |
| Tiltakstype: | Administrativt/teknisk | Uautorisert tilgang til systemet.  Administrator-tilganger slettes ikke når administrator slutter i stillingen. Ref. punkt 7 over h(tiltakskort nr. 6). | Rollestyrt tilgang, begrense administrator rettigheter. |
| Risikoelement: | **8** |
| Risikonivå: | **Middels** |
| Anm: | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Tiltakskort nr. 8** | |  |  |
| Organisasjon: | NTNU | Risiko | Tiltak |
| Tiltakstype: | Administrativt/teknisk | Uvedkommende får tilgang til sensitive data  Brukernavn og passord på avveie, fanges opp pga. at O365 er tilgjengelig fra internett. For eksempel dersom man sitter på en internettcafe, kan det være skadevare på denne maskinen som brukeren ikke har kontroll over. (key-logger) | Policy-basert lagring, informasjon og brukeropplæring |
| Risikoelement: | **15** |
| Risikonivå: | **Middels** |
| Anm: Etablert løsning for varsling av slike hendelser i O365 | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Tiltakskort nr. 9** | |  |  |
| Organisasjon: | NTNU | Risiko | Tiltak |
| Tiltakstype: | Administrativt | Uvedkommende får tilgang til sensitive identitetsdata  Data om personer med skjult identitet kan blit tilgjengeligjort gjennom Office365 | Bevisstgjøring av brukere |
| Risikoelement: | **17** |
| Risikonivå: | **Middels** |
| Anm: | |

# Vedlegg A Kopi av ROS-regneark





# Kommentarer fra deltakerne

**Fra:** Snorre Jensen <[snorre@enable.no](mailto:snorre@enable.no)>  
**Dato:** 31. mai 2016 kl. 15.15.41 CEST  
**Til:** Ole Ingvard Langfeldt <[ole.langfeldt@ntnu.no](mailto:ole.langfeldt@ntnu.no)>  
**Kopi:** Kirsti Sørgaard Moe <[kirsti.moe@ntnu.no](mailto:kirsti.moe@ntnu.no)>  
**Emne:** **SV: Risikovurdering av Office 365, Sharepoint, OneDrive - Brukerperspektiv deling**

Jeg har en generell tilbakemelding på feltet «Sannsynlighet» og det er at det nok generelt ligger for høyt. Dette grunnet en mengde på 46000 brukere med den skalaen som lå til grunn. (ukentlig, årlig, hvert 5 år etc…) Tror dette bør være med som en generell merknad til eventuell rapport. Ser på nett at man i lignende situasjoner kalkulerer sannsynlighet basert på % sannsynlighet for et enkeltindivid og ganger opp med et fornuftig forhåndsdefinert tall. (Men forskjellig praksis er å finne rundt dette)

Jeg har ingen vesentlige tilføyinger til risikoanalysen utover at det bør gjøres et godt stykke arbeid for å adressere risikoreduserende tiltak i større grad. Mener vi bør sette oss ned sammen på NTNU og følge opp dette.

Når det gjelder utfordringen knyttet til plassering av data i utlandet så anbefaler jeg at Microsoft i Norge utfordres på dette. Jeg har snakket med Lasse Finsås hos Microsoft om dette og han sier at han kan bidra i å tydeliggjøre dette slik at man har bedre innsikt i hvilke typer data som potensielt kan lagres hvor. Tror at dette vil kunne redusere risikoen knyttet til dette punktet. Gi beskjed om dere ønsker at jeg skal få noe mere konkret om dette fra Microsoft.

Vennlig hilsen

Snorre Jensen

**Fra:** Ole Ingvard Langfeldt <[ole.langfeldt@ntnu.no](mailto:ole.langfeldt@ntnu.no)>

**Emne: Re: ROS - O365 - Epost**

**Dato:** 2. juni 2016 kl. 15.23.50 CEST

**Til:** Hildegunn Vada <[hildegunn.vada@uninett.no](mailto:hildegunn.vada@uninett.no)>

Har ikke noe svar til deg nå.

Men Microsoft har kommet tilbake til meg  ang ROS en vi har hatt. De mener at vi ikke har forstått alt som har skjedd i det siste. Interesant. Det er viser egentlig på det som  vi snakket om. Forvaltning og drift. Jeg skal se om jeg får møte med dem den 14 juni.   
  
Vennlig hilsen

Ole Langfeldt