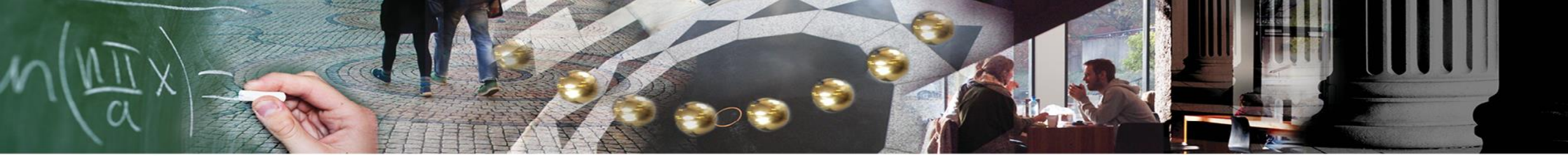

UiO : Universitetet i Oslo

Sikkerhet ved outsourcing

Espen Grøndahl

IT-sikkerhetssjef

UiO

Agenda

- Sikkerhet - hva er det egentlig?
- Uønskede hendelser
- Hva må en huske på?
- Tør vi dette da?

Sikkerhet

"Sikkerhet kan defineres som en tilstand; fravær av uønskede hendelser eller frihet fra fare og frykt. Denne tilstanden er imidlertid ikke statisk, men påvirkes av endringer i faktorer som trussel og farer, sårbarhet og verdi. " - Store Norske Leksikon

Uønsket hendelse, hva er nå det da?

- Tap av data
- Tap av renommé
- Økonomisk tap – eller erstatningsansvar
- Tap eller fare for liv

SIKKERHET VED OUTSOURCING

Hva bør vi tenke på

- Hvilke data?
- Hvordan flyter data?
- Hva skal de brukes til?
- Brukerhåndtering og tilganger
- Merkantile forhold
- Juridiske forhold
- Oppdateringer, endringer og vedlikehold
- Driftsmiljø
- Revisjon og tilsyn

Hvilke opplysninger skal overføres?

- Personopplysninger
- Sensitive personopplysninger
- Arkivpliktige opplysninger
- Regnskapsdata
- Bedriftshemmeligheter
- Andre data av stor verdi
- Data underlagt eksportkontroll

Hvordan flyter data?

- Hvilke data overføres hvordan? Og når? Kryptert?
- Informasjon om brukerne?
  - Brukernavn, fullt navn, e-post, telefonnummer
  - Provisjonering – ved bruk, eller i bulk.
- Autentisering?
  - Synkronisering av passord
  - SAML2, FEIDE, Dataporten, LDAP, AD
- Autorisasjon
  - Grupper, roller? Manuelt eller fra kildesystem
  - Hvordan oppdateres disse? Finnes historikk?
- Flyter data tilbake?
  - kan det indirekte påvirke sikkerheten på lokale løsninger?

Hva benyttes data til?

- Benyttes de kun til ditt formål, og innenfor det avtalene tillater?
  - Er det spesifisert godt nok?
  - Kan det skje endringer over tid?
  - Har alle parter den samme oppfatningen av avtalen?
- Kan leverandøren benytte data til eget formål?
  - Forbedring av tjenestene
  - Til reklame / markedsføring
  - Kan data selges til tredjepart?
  - Til profilering av brukerne?

Brukerhåndtering og tilganger

- Innrullering, avslutning og sperring
  - Hvordan gis tilgang?
  - Hvordan fjernes tilganger?
  - Kan en sperre en bruker ved tap av passord, eller mistanke om misbruk?
- Tilgangskontroll
  - Sporing av endring
  - Sporing av bruk
  - Avdekke uautorisert bruk
  - Tilgang for driftspersonell

Merkantile forhold

- Eierstrukturer hos leverandør
- Lisenser – gratis er ikke alltid gratis, må det ut på anbud?
- Underleverandører - I flere ledd og over landegrenser?
- Bruksvilkår - "fair use"
- Eierskap til data
- "Exit-strategi"
- SLA? Tjenestekvalitet? Sanksjoner?
- Avvikshåndtering - setter avtalene begrensninger?

Juridiske forhold

- Databehandleravtaler
- Risikoanalyser
  - Er systemet innenfor akseptabel risiko?
  - Hvem eier denne risikoen? Du som kunde, eller sluttbruker?
- Lovlig grunnlag for å overføre data til utlandet
  - EU/EØS? USA? Andre?
- Formåls- og hjemmelsvurderinger
  - Hva skal systemet brukes til?
  - Finnes det lovhjemmel for å samle inn personopplysninger til dette?
- Personvern
  - Innebygd personvern
  - Trygge standard-innstillinger

Oppdateringer, endringer og vedlikehold

- Hvordan oppdateres tjenesten?
  - Kontinuerlig? Varsles det? Kan du som kunde styre det?
  - Kan endringer utløse endringer i avtaler eller risikoanalyser?
  - Kan det avtales rammer som det kan endres innenfor?
- Sikkerhetshendelser
  - Hvordan vil du som kunde bli varslet?
  - Har du muligheter til å avdekke det selv?
  - Tilgang til logger?
  - Tilgang til leverandør? Er du en liten kunde hos en stor leverandør?

Driftsmiljø

- Serverhaller? AWS? Azure?
- Backup?
- Hvordan holdes data separat fra andre kunder?
- SLA – oppetid?
- Tilgang til data
  - Fra driftspersonell
  - Fra utenlandske myndigheter
  - Fra underleverandører
- Har du tilgang på logger?

Revisjon og tilsyn

- Hvordan sikrer du at leverandøren overholder alle krav?
- Kan du føre tilsyn? Kan du teste sikkerheten?
- Tredjepartstilsyn?
  - Tilgang på rapporter
  - Muligheter ved avvik
- Sertifiseringer
  - ISO 27001
  - ITIL
  - Hva er dekket? Og hva er "reklame"?

Tør vi dette da?

Hvor godt kontroll har du "egentlig" in-house?

- Teknisk sikkerhet
  - Er alt fullt patchet alltid?
  - Full kontroll på brukertilganger
  - Konfigurert etter "best practices"
  - Tilgang til maskinrom
  - Backup / restore
  - Tilgang til kompetanse, ressurser og tid internt
- Merkantilt/juridisk
  - Alle avtaler er på plass og arkivert
  - Risikoanalyser er oppdatert

Det hele handler om risiko

- Hvilken risiko er vi villige til å ta?
  - Tar vi risiko selv, eller på vegne av andre?
  - Er den innenfor det vi kan akseptere?
  - Tas denne avgjørelsen av rett person?
- Er de tingene vi er redd for innenfor trusselmodellen vår?
  - Er NSA ute etter julebordspåmeldingene våre?
  - Veldig fort gjort å bli **for** redd for de feil tingene.

Oppsummering

- Fullt mulig å outsource mange tjenester
  - Noen vil kreve mer enn andre
- Neppe ønskelig eller mulig å komme utenom outsourcing
  - De færreste vil ha økonomi eller ressurser til å drive alt selv
- Velg de rette tjenestene å sette ut
  - Rett for din virksomhet, basert på strategi, økonomi og kompetanse
- Gjør ”papirarbeidet” – avtaler, jus og risikoanalyser
- Følg opp leverandørene!
  - Benytt avtalene, si i fra ved brudd og sjekk at de følges.

Spørsmål?