RT 411881

2021-01-05 16:01:59 **lenaf (Lena Charlotte Finseth)** -

Date: Tue, 5 Jan 2021 15:01:47 +0000
CC: "'fs-core'" <fs-core@admin.uio.no>
Subject: [Fs-support] Mer loggføring og kontrollrapporter i FS?
To: "fs-support@unit.no" <fs-support@unit.no>
From: "Lena Charlotte Finseth" <l.c.finseth@admin.uio.no>

Hei

Forvaltningen av Felles studentsystem (FS) ved Universitetet i Oslo (UiO) ble høsten 2019 revidert av UiOs Enhet for intern revisjon (EIR). Formålet med revisjonen var å vurdere systemets internkontroll. Forslag til tiltak inngår i Årsrapport 2019 - Enhet for internrevisjon. Universitetsstyret ved UiO tok i møte 10. mars 2020 internrevisjonens årsrapport til etterretning, og ba administrasjonen følge opp de foreslåtte tiltakene og rapportere tilbake til universitetsstyret.

Avdeling for studieadministrasjon (studieavdelingen) på UiO har fått ansvar for å følge opp de foreslåtte tiltakene med Unit, som leverer FS. EIRs rapport konkluderer med at det bør vurderes om man kan gjøre kompenserende kontroller på områder der enkeltpersoner har sterke rettigheter, for eksempel at det gjennomføres periodiske stikkprøvekontroller av grunnlaget for endring av karakterer eller oversendte data til DBH.

Logging

EIRs viktigste konklusjoner gjelder personvern knyttet til manglende logging. Alle 600 FS-brukere på UiO har lesetilgang til data på tvers av fakultet. Men det er ikke rutiner for å avdekke mulig uautoriserte oppslag. Den nye personvernforordningen (GDPR) har skjerpet krav til virksomhetens eget ansvar for å ivareta personvern. EIR vurderer at det er risiko for uautorisert tilgang til data. Tilganger blir logget, men det er ikke utviklet rutiner for kontroll for å avdekke eventuell misbruk av tilganger.

Det er ikke et eksplisitt krav i personvernlovgivingen fra 2018 at UiO må fremvise hvilke personer som har vært inne på studenten i systemet, dersom studenten etterspør det. Det er kun hvilke grupper (kategorier) av personer som har fått se opplysninger som personvernlovgivingen krever at UiO må kunne gi innsyn i. Personvernlovgivingen krever likevel at UiO har tilstrekkelig internkontroll som sikrer at personopplysninger blir behandlet lovlig, sikkert og forsvarlig. Juristene på Universitetets senter for informasjonsteknologi (USIT) påpeker at å føre logg over hvem som har sett personopplysninger i FS, vil kunne bidra til å oppfylle GDPRs krav til integritet og konfidensialitet.

EIR mener rutinene bør forbedres, fordi det bør være mulig i ettertid enkelt å kontrollere logger over hvilke personer/identiteter, i hvilket omfang og tidspunkt, de har sett på eller endret data eller personopplysninger. Behovet er å etablere rutiner og kontroller av unormale hendelser for å avdekke bevisste eller ubevisste feil eller uberettigede oppslag (snoking) i FS.

Dagens status og muligheter

Dersom det etter hvert blir slik at personopplysninger av særlig kategori kan lagres direkte i FS, må Unit vurdere ekstra loggføring og tilgangsstyring. Dette er antagelig noe Unit selv har tenkt på og planlagt med. Vi ønsker å få på plass retningslinjer som sier at all tilgang til særlige kategorier og liknende krever MFA (multifaktor-autentisering / 2-faktor ved innlogging, som f.eks. SMS med engangskode, app på mobiltelefon, innlogging med bank-id eller tilsvarende). Vi mener at Unit bør få støtte for MFA inn i planene.

Ved UiO baserer vi oss per i dag på tillit og opplæring. Vi har nettsiden "Taushetsplikt og snoking i FS" [https://www.uio.no/for-ansatte/arbeidsstotte/sta/fs/tilgang/taushetsplikt-og-snoking.html [Open URL]] som alle FS-brukere må gjøre seg kjent med. Studieavdelingen har vurdert tiltak for å hindre snoking ved hjelp av mer logging og mer lesebegrensning i Felles studentsystem (FS) på UiO. Det er hensyn som taler både for og imot, og vi er usikre på om utstrakt logging av alle oppslag vil være den eneste måten å få avdekket misbruk av dagens tillitsbaserte rutiner. Vi er interessert i å høre fra Unit om dere ser bedre tiltak for å ha kontroll til enhver tid, fortrinnsvis før misbruk har funnet sted.

Per januar 2021 er FS slik at systemeier kan ta ut logg på hvor mange ganger en FS-bruker har åpnet en FS-rapport, en FS-rutine og et FS-bilde, men vi kan ikke se hvilke opplysninger FS-brukeren har søkt opp og dermed hvilke opplysninger om hvilke personer vedkommende har hatt mulighet til å se, og ev. videreformidle urettmessig til utenforstående.

Dersom FS-brukeren har endret på dataene, blir det ikke logget mer enn det vi kan se i FS-klienten. En rekke av bildene i FS viser allerede i dag hvem som har lagret en endring og når, enten ved hjelp av en rutine, som kan endre data på mange studenter på én gang ved hjelp av ett tastetrykk (oppdatering ved rutinekjøring eller nattjobb), eller ved manuell endring direkte i et bilde på én og én person av gangen, eller ev. via SQL. Vi ser at det ville være nyttig med mer utstrakt logging av endringer, slik at systemeier kan finne og dokumentere dem ved for eksempel mistanke om uautorisert endring av opplysninger eller også kunne avkrefte og dokumentere at slik uautorisert endring ikke har funnet sted av en gitt FS-bruker i forbindelse med mistanke om for eksempel korrupsjon.

Per i dag er det slik at dersom en FS-bruker for eksempel åpner en rapport/rutine/bilde om morgenen, uten å lagre nye data, og så har rapporten/rutinen/bildet åpent hele dagen og gjør flere søk, blir dette loggført kun som én åpning. Vi har derfor ikke oversikt over nøyaktig hvilket utplukk en ansatt har fått tilgang til.

Logg av hva en FS-bruker leser i FS vil være et viktig verktøy i behandling av typiske avvikssaker. Enten det er saker med datainnbrudd, hvor brukernavn/passord har kommet på avveie og utenforstående har fått tilgang til FS så vi trenger å kartlegge hvilken informasjon som er kommet på avveie, eller saker med utro tjenere og tilsvarende, hvor slike logger kan brukes i etterkant av en hendelse eller ved mistanke om en hendelse.
Logg av lesing vil også gjør det mulig å sette opp overvåkning for å forsøke å avdekke misbruk av rettigheter.

Det blir ikke logget dersom data er hentet ut av FS og f.eks. lagret utenfor FS, utenfor de ulike integrasjonsløsningene som finnes ut og inn av FS. Vi syns det ville være nyttig og antagelig et overkommelig tiltak å innføre slik logging, både med tanke på å avdekke uautorisert bruk av data og i opplæringsøyemed og til kontrollformål.

Innvendinger mot mer logging

Studieavdelingen ser imidlertid at loggføring av alle søk selv uten oppdatering ville utgjøre en enorm mengde data. Vi har vært tvilende til om muligheten for å avdekke og dokumentere et uautorisert oppslag ville forsvare loggføring og lagring av hele datamengden. Vi har derfor sett nærmere på dette, og ser at UiO sitt loggsystem er fint skalert til å kunne motta og håndtere full leselogg fra FS. Dersom en bruker leser info om student X i FS, er det imidlertid ikke nødvendig med logg på all data om student X, bare å få logget at brukeren har sett på data om student X. Vi har både hjemmel og nødvendig formål på plass for å gjøre dette for sikkerhet. På UiO er standard lagringstid for logger 12 uker (ca. 3 måneder), men for dette formålet vil vi sammen med behandlingsansvarlig vurdere om det kan være behov for kortere eller lenger lagringstid. Tiden må kanskje være tilstrekkelig lang til å avdekke systematisk misbruk over en viss tid. Blant alle risikomomenter utgjør ikke-tillatte oppslag blant FS-brukerne med autorisert tilgang kun én av farene for at data kommer på avveide. På den annen side vil ikke slik god logging innenfor ett risikomoment være til hinder for andre tiltak i tillegg, som for eksempel å hindre uautorisert tilgang til FS.

Hensynet til å kunne dokumentere snoking mot hensynet til å unngå overvåking av ansatte må også gås opp. Her kan studieavdelingen på UiO i første omgang konsultere og konferere med avdelinger på UiO som arbeider med slike vurderinger.

Et alternativ til utstrakt logging av oppslag kunne være å begrense lesetilgang til f.eks. enheten den ansatte jobber på eller til for eksempel aktive studenter.
En slik begrenset lesetilgang vil imidlertid kunne

- hindre tjenestemessig behov for å sammenlikne data, for å sikre en helhetlig registreringspraksis.
- hindre tjenestemessig behov for å ha oversikt over studenter som tar emner på ulike fakulteter og institutter. Særlig på bachelorprogrammene er det krav om både dybde og bredde i emnevalg, og gjerne på tvers av fakulteter.

- hindre mulighet til bred og individbasert studieveiledning basert på studentens tidligere studieløp

Det vil også være slik at om man begrenser lesetilgang i større grad enn i dag, vil det ikke hindre eventuelt misbruk knyttet til de opplysningene den ansatte har tilgang til.

Vi har med dette presentert noen problemstillinger og foreslått noen konkrete tiltak. Vi ber Unit vurdere mulige løsningsalternativer. Kan vurderingen eksempelvis inngå som del av arbeidet etter Gartner-rapporten med å fornye FS?

Hilsen
Studieavdelingen ved UiO
ved Lena Finseth

2021-01-15 10:08:58 **knutlov (Knut Løvold) - Correspondence added**

Hei, da har vi hatt en runde her angående dette.

Som jeg ser det er det her flere ulike problemstillinger.

1. **Multifaktor-autentisering**.
Så vidt jeg har forstått er det mulig å legge inn to-faktor-autentisering i Feide, dvs. at man kan kreve to-faktor for å logge inn i UH-kiosken, for å kunne logge inn i FS. Da tenker jeg at dette er en løsning som vil kunne fungere foreløpig, men at dette selvfølgelig blir en del av moderniseringsprosjektet å ha innloggingsløsninger som dekker alle krav til sikkerhet.

2. **Logging av endringer**.
Her er det allerede mye som logges, men det er ikke noe i veien for å utvide denne loggingen, bare vi får beskrevet hva som skal logges.

3. **Logging av oppslag, uten endring**.
Det er vel dette som er hovedproblemstillingen i forhold til snoking. Her er logging langt mer problematisk i forhold til å kunne avdekke ureglementert bruk. Oppslag kan gjøres ved:

A. Kjøring av en rapport.
Det er mulig å logge hvem som har kjørt en rapport og hvilke utplukkskriterier som er benyttet. Man kunne jo også logge også resultatet, men det ville medføre en enorm mengde logget data. Logger man ikke innholdet, vil man ikke nødvendigvis klare å gjenskape innholdet, fordi grunnlagsdata kan være endret. F.eks. kan en studierett være gått ut, slik at en person ikke lenger kommer i en liste.

B. Oppslag i bilder.
Oppslag kan gjøres både på enkeltpersoner eller grupper av personer. F.eks. kan man søke fram alle på et kull. Igjen vil det bli svært mye logging dersom man skal angi på hver enkelt person at de er hentet opp. Alternativt skal man ikke logge før man faktisk blar, slik at personinformasjon vises i bildet. Det vil kunne være teknisk vanskelig, fordi det i enkelte tilfeller må ta hensyn til størrelsen på skjermen. Typisk ville det også bli svært mange logginger på de som kommer først i et utplukk. Må man kunne skille på hva som kunne vært sett på, og det som faktisk er sett på? Skal man mistenkes for snoking, fordi en kjendis tilfeldigvis er i et utplukk, men man aldri har sett på vedkommende? Skal det tas hensyn til å logges hvor lenge man har en person oppe i bildet? Slike krav vil uansett kunne omgås ved å ta skjermbilder, eller mobilfoto av skjermen. En tredje mulighet er er å logge søkekriteriet i bilder, f.eks. at man har søkt på et kull. Gir også store logger, men på langt nær det som en logging av enkeltpersoner vil gi. Som UIO er inne på er kanskje ikke logging det som er løsningen men flere begrensninger i lesetilgang, og et fortsatt tillitsbasert system.

Knut