



Universitetet i Bergen

Rapport fra gjennomgang av valgavvikling

Bergen, 19.05.2009

 **ERNST & YOUNG**

Rapporten skal kun benyttes av Universitetet i Bergen til de formål den er ment og skal ikke distribueres til andre parter uten vårt skriftlige samtykke. Rapporten er ment som en oppsummering av vårt arbeid med gjennomgang av valgavviklingen. Ernst & Young er kun ansvarlig for rapportens innhold ovenfor Universitetet i Bergen. Vi viser for øvrig til avtalte ansvarsbegrensninger.

Innledning (1/2)

Bakgrunn

Universitetet i Bergen (UiB) gjennomførte en elektronisk avstemming for valg av rektor i tidsrommet 27. mars til 2. april 2009. Under valget avdekket UiB uregelmessigheter ved at personer hadde avgitt ugyldige stemmer.

Det ble besluttet at IT-avdelingen skulle gå inn i valgdata og identifisere de ugyldige stemmene. IT-avdelingen fant at 4 personer hadde avgitt ugyldige stemmer. 2 studenter hadde avgitt flere stemmer ved en feiltakelse, mens 2 studenter hadde i samarbeid med professor i Informatikk testet ut svakheter i valgsystemet. Denne testen ble utført på eget initiativ og uten godkjenning fra administrasjonen.

Valget ble avsluttet 2. april og valgstyret gikk gjennom protokoll for valget. Valgstyret besluttet å offentliggjøre uregelmessighetene ved valget, og informerte de to kandidatene før offentliggjøring.

I brev datert 13. april 2009 reiser Rolf Reed og Ernst Nordtveit problemstillinger til den tekniske gjennomføringen av rektorvalget med hensyn til sikkerheten. Brevskriverne stiller spørsmål ved tilgangen til stemmesedler og uregelmessigheter i stemmelogg og stemmesedler.

IT-avdelingen har redegjort for hvem som har tilgang til valgdata og hvem som har benyttet tilgangene. Resultatet av dette arbeidet er presentert for ledelse og styre ved UiB.

Den 15. april kontaktet UiB Ernst & Young for å få en uavhengig gjennomgang av de spørsmålene brevskriverne har stilt. Ernst & Young gjennomførte i 2008 en internrevisjon av Mi side som studentportal. Det var derfor naturlig å be Ernst & Young om å gjennomføre en tilleggsrevisjon som omfattet valgsystemet. Dette dokumentet oppsummerer resultatet av Ernst & Young sin gjennomgang.

Universitetsstyret hadde valget til behandling 30. april og tok fremlagt valgprotokoll og redegjørelse fra universitetsdirektøren til etterretning.

Om valgsystemet

UiB startet med elektroniske valg i 2005. Ved valg av rektor i 2005 ble det benyttet en ekstern programvare fra NTNU. Ved etterfølgende valg ble valgmodulen ("survey-modulen") i Mi side benyttet. Valgmodulen er en tilleggstjeneste som er utviklet for meningsmålinger i Mi side. UiB holdt det første elektroniske valget ved bruk av valgmodulen i 2005 der Universitetsstyret ble valgt.

Valgmodulen brukes i dag til meningsmålinger og valg. Det er gjort tilpasninger i valgmodulen med den hensikt å bedre sikkerheten ved rektorvalget og andre valg der høyere sikkerhet er ønsket.

Mi side lagrer sine data i en database. Valgdata er lagret i en tabell i den samme databasen hvor øvrige data i Mi side lagres. Tilgangsrettigheter til databasen skiller ikke mellom valgdata og øvrige data.

Innledning (2/2)

Om rektorvalget

Valget ble gjennomført i perioden fra 27. mars kl 1000 til 02. april. kl 1600. Kandidatene til valget var:

- ▶ Sigmund Grønmo (rektorkandidat) og Berit Rokne (prorektorkandidat)
- ▶ Rolf K. Reed (rektorkandidat) og Ernst Nordtveit (prorektorkandidat)

Manntallet avga sine stemmer på kandidatene gjennom valggrupper. Det ble opprettet fire valggrupper basert på stemmegivernes stilling og posisjon på UiB.

Formål

Formålet med Ernst & Young sin gjennomgang er å gi UiB et uavhengig svar på de spørsmål som er stilt i brevet av Reed og Nordtveit. Følgende spørsmål fremgår i brevet:

- ▶ Hvem har hatt mulighet for tilgang til dataene under valget?
- ▶ Hvem har faktisk vært inne og sett på dataene?
- ▶ Hvilke sikkerhetssystemer er lagt inn for å sikre at ingen uautoriserte får adgang og for å kunne etterspore hvem som har vært inne?

Forutsetninger og begrensninger

Rapporten er basert på intervjuer av 15 sentrale personer i forhold til valgavviklingen. Personene omfatter representanter for ledelsen, valgstyret, IT-avdelingen, Utdanningsavdelingen, professor i Informatikk og studenter. Ernst & Young har fått snakke med alle de personene som vi mener har vært nødvendig for å svare på spørsmålene.

I tillegg har Ernst & Young fått tilgang til elektroniske logger i tidsrommet 27. mars til 2. april 2009, samt annen relevant dokumentasjon.

Ernst & Young forutsetter at mottatt informasjon er korrekt. Det vil likevel alltid være en risiko for at forhold som kunne ha medført ytterligere observasjoner, eller en annen konklusjon, ikke har vært vurdert.

Vår gjennomgangen av valgavvikling omfatter de formelle og etablerte prosessene for tilgang til valgdata og omfatter ikke bakveier eller tilgang til valgdata gjennom innbrudd eller andre uautoriserte prosesser.

Vi har ikke gjennomført en risikovurdering, sårbarhetsanalyse eller trusselvurdering av valgsystemet eller valget. Vi har ikke gjort en vurdering av valgsystemet eller valgavviklingen opp mot personvern generelt eller Personopplysningsloven spesielt.

Vi har ikke gjennomført en valideringsanalyse eller annen form for verifisering av valgdatas integritet.

Gjennomgang av valgavvikling (1/4)

Hovedoppsummering

Basert på vår gjennomgang av valgavviklingen er det 21 personer som har hatt mulige tilganger til ulike data under valget. Det er ingen vedtak eller styrende dokumenter som angir hvem eller hvor mange som skal ha tilgang til valgdata.

Basert på gjennomgang av elektroniske logger i valgperioden har 2 personer lest anonymiserte valgdata.

Basert på gjennomgang av elektroniske logger i valgperioden fremgår det at 5 personer har hatt mulighet for å lese og endre valgdata. Alle 5 personene er ansatt ved IT-avdelingen. Gjennom intervjuer har 4 personer opplyst at de ikke har vært inne i valgtabellen. Ernst & Young har ikke mulighet for å bekrefte dette, da det ikke finnes elektroniske logger for aktivitetene.

1 person bekrefter å ha vært inne i valgtabellen med tilgang til både å lese og endre ikke-anonymiserte valgdata. Denne personen sier i intervju at dette ble gjort etter henvendelse fra valgstyret etter at det ble identifisert uregelmessigheter ved valget. Ernst & Young har ikke mulighet for å etterspore hvilke aktiviteter som har vært utført i valgtabellen, da det ikke finnes elektroniske logger for aktiviteter i valgdata.

Gjennom intervjuer har vi ikke funnet at noen har brukt sine rettigheter til å endre valgdata. Gjennom intervjuer har vi funnet at 4 studenter har avlagt ugyldige stemmer. Ernst & Young kan ikke bekrefte at integriteten i valgdata er ivaretatt, da det ikke finnes elektroniske logger for aktiviteten i valgdatabasen.

UiB har ikke etablert formelle rammeverk rundt valgsystemet, som risikoanalyse, sårbarhetsanalyse, trusselvurdering samt styrende dokumenter. Ernst & Young kan derfor ikke konkludere på om det er tilstrekkelig sikkerhet i valgsystemet.

Gjennomgang av valgavvikling (2/4)

Spørsmål	Observasjon
Hvem har hatt mulighet for tilgang til dataene under valget?	<p data-bbox="719 389 2033 416">Basert på intervjuer og gjennomgang av elektroniske logger fra perioden 27. mars til 2. april 2009 har vi funnet:</p> <ul data-bbox="719 443 1951 643" style="list-style-type: none"><li data-bbox="719 443 1368 470">▶ 1 person har tilgang til å lese anonymiserte valgdata<li data-bbox="719 497 1951 525">▶ 7 personer har tilgang til å lese ikke-anonymiserte valgdata samt avlegge stemmer på vegne av andre<li data-bbox="719 552 1570 579">▶ 11 personer har tilgang til å lese og endre ikke-anonymiserte valgdata<li data-bbox="719 606 1794 633">▶ 2 personer har tilgang til historiske ikke-anonymiserte valgdata gjennom sikkerhetskopier <p data-bbox="719 660 2033 699">Det er ingen vedtak eller styrende dokumenter som angir hvem eller hvor mange som skal ha tilgang til valgdata.</p>

Gjennomgang av valgavvikling (3/4)

Spørsmål	Observasjon
Hvem har faktisk vært inne og sett på dataene?	<p data-bbox="714 384 2018 411">Basert på intervjuer og gjennomgang av elektroniske logger i perioden 27. mars til 2. april 2009 har vi funnet at:</p> <ul data-bbox="714 443 2051 1394" style="list-style-type: none"><li data-bbox="714 443 1944 512">▶ 2 personer har i valgperioden lest anonymiserte valgdata. Disse personene har sett hele eller deler av valggruppene samlede stemmer fordelt på kandidatene i valget.<li data-bbox="714 544 2051 767">▶ 2 personer har vært inne i databasen til Mi side i valgperioden. De 2 personene har fulle tilganger til å lese og endre ikke-anonymiserte valgdata. Det er ikke mulig å etterspore hva disse personene har gjort da de var inne i databasen. De 2 personene er ansatt i IT-avdelingen, og har i følge IT-avdelingen sine oppgaver knyttet til databasen til Mi side. Gjennom intervjuer bekrefter den ene å ha vært inne i valgtabellen i valgperioden etter anmodning fra sekretær for valgstyret, for å identifisere de ugyldige stemmene. Den andre sier i intervjuer at han ikke har vært inne i valgtabellen.<li data-bbox="714 799 2051 906">▶ 1 person deler brukeridentitet med den personen som har vært inne i valgdatabasen. Gjennom intervju opplyser personen at han ikke har vært inne i databasen i valgperioden. Ved bruk av felles brukeridentiteter er det ikke mulig å identifisere hvilken person som faktisk har vært inne i den gitte perioden.<li data-bbox="714 938 2051 1123">▶ I tillegg har 2 personer i valgperioden vært pålogget serveren der Mi side er lagret. Det er teknisk mulig for disse 2 personene å få adgang til valgdata gjennom en inngangsport fra serveren uten at dette registreres i elektroniske logger. I intervjuer med disse 2 personene sier de at de ikke har benyttet muligheten til å lese eller endre valgdata. Det er imidlertid ingen elektroniske logger som kan bekrefte dette. De 2 personene er ansatt ved IT-avdelingen, og i intervjuer sier de at deres arbeidsoppgaver er knyttet til Mi side serveren.<li data-bbox="714 1155 2051 1257">▶ Det er 8 personer som har mulighet til å benytte en annen persons brukeridentitet i Mi side. Disse kan lese hva andre brukere har stemt samt avlegge stemmer på vegne av andre. Gjennom elektroniske logger har vi ikke funnet at dette har forekommet.<li data-bbox="714 1289 2051 1394">▶ 2 studenter har i samarbeid med en professor i informatikk testet ut svakheter i valgsystemet. De bekrefter selv at de ikke har vært inne i valgsystemet eller hatt uautoriserte tilganger, men at de kun har hatt tilgang til å avlevere flere stemmer.

Gjennomgang av valgavvikling (4/4)

Spørsmål	Observasjon
Hvilke sikkerhetssystemer er lagt inn for å sikre at ingen uautoriserte får adgang og for å kunne etterspore hvem som har vært inne?	<p>Formelle policyer og prosedyrer</p> <p>For å kunne vurdere tilstrekkelig sikkerhet i et valgsystem bør følgende rammeverk være formalisert (listen er ikke uttømmende):</p> <ul style="list-style-type: none">▶ Det bør være utarbeidet en risikovurdering eller risikoanalyse, en trusselvurdering eller sårbarhetsanalyse, samt en kravspesifikasjon til valgsystemet.▶ Det bør være klare vedtak eller styrende dokumenter som angir hvem som skal ha tilgang til valgdata.▶ Det bør være en formalisert prosess som angir når eller hvordan velgernes anonymitet kan brytes. <p>Vi kan ikke konkludere om det er tilstrekkelig sikkerhet i valgsystemet da nevnte vurderinger og rammeverk ikke er etablert.</p> <p>Kontroller for tilgang til Mi side og valgdata</p> <p>Følgende sikkerhetssystemer er implementert i Mi side og valgsystemet:</p> <ul style="list-style-type: none">▶ Det er krav til brukernavn og passord for tilgang til valgdata. Krav til passordets oppbygging følger øvrig passordpolicy gjennom ordinær brukeradministrasjon. Krav til passord er ikke knyttet opp mot en risikovurdering av krav til passord mot et valgsystem.▶ Det er delvis aktivert logging av brukeraktivitet. Logging er ikke altomfattende for alle brukere og all brukeraktivitet. Sporbarhet er derfor ikke fullstendig. <p>IT-teknisk utfordring</p> <ul style="list-style-type: none">▶ Det har vært teknisk mulig å avgi flere stemmer ved et uhell samt ved bevisst å avlegge ugyldige stemmer. IT-avdelingen arbeider med å utbedre feilene, og en korrigering ligger klar til testing.

Ernst & Young
Bergen, 19.5.2009

A handwritten signature in black ink, reading "Anita Meidell". The script is cursive and fluid, with the first letters of the first and last names being capitalized and prominent.

Anita Meidell
Partner

Ernst & Young

Assurance | Tax | Transactions | Advisory

Om Ernst & Young

Ernst & Young er en ledende global aktør innen revisjon, skatt og avgift, transaksjoner og rådgivning. Våre 135 000 ansatte verden over - 1 400 i Norge - har et sterkt fellesskap bygget på felles verdier og et kontinuerlig fokus på kvalitet. Vi bidrar til at våre medarbeidere, kunder og samfunnet rundt oss realiserer sitt potensial.

www.ey.no

© 2009 Ernst & Young AS
All Rights Reserved

