Klassekampen
3/2-2010

Er elektronisk valg trygt?

VALG 2011

Hans Ekkehard Plesser

Kommunal- og regionaldepartementet (KRD) fortjener ros for åpenheten rundt eValg 2011: Mange saksdokumenter er tilgjengelig på prosjektets hjemmeside (http://bit.ly/5HLNYa) og prosjektet bygger på programvare med åpen kildekode. Det er betryggende at professor Kjell Hole langt på vei går god for løsningen i Aftenposten 25.1. Men en rekke spørsmål gjenstår.

Både KRD og Hole lover at eValg systemet skal sikre frie og hemmelige valg, selv når det stemmes fra virusinfiserte PC-er. Dessverre antydes bare hvilke teknologier som skal brukes til dette — her trenger vi straks omfattende forklaringer som er forståelig for lekfolk.

Vil systemet kunne sikre hemmelig stemmegivning selv hvis såkalte keyloggere, som fanger opp ethvert tastetrykk, er installert? Hvordan fungerer kvitteringene? Ifølge Hole skal valgkortet inneholde personlige koder for hver velger og parti. Etter at du har stemt, får du en kvittering per SMS med en kode. Står samme kode på valgkortet ved siden av partiet du ville stemme på, er du trygg på at stemmen din er registrert riktig. Men hva hvis noen avlytter datatrafikken til valgkorttrykkeriet og SMS som sendes ut? Vil den ikke da kunne finne ut hva du har stemt?

I valglokaler passer funksjonærer på at den enkelte får gi sin stemme fritt i valgavlukket. Denne kontrollen faller bort straks du stemmer på PC. For å sikre fritt valg, skal du derfor kunne stemme elektronisk så ofte du vil og stemmen som du avgir i valglokalet vil ha forrang foran elektronisk avgitt stemme. Men finnes det sosialvitenskapelig forskning som viser at denne mekanismen vil fungere i praksis? I dag må alle som vil stemme, oppsøke valglokalet og får klar beskjed om å gå inn i avlukket en og en. Ved elektronisk valg kan du havne i en situasjon der du må rettferdiggjøre at du vil gå til valglokalet: Hvorfor skulle du dit med mindre du ønsket å stemme annerledes enn du skal?

Avslutningsvis to anmerkinger til kontrakten for eValg-systemet, som ble tildelt ErgoGroup i desember: ErgoGroup sitt tilbud var bare halvparten så dyrt som de to konkurrerende tilbud. Hvordan klarer Ergo det? Eller ligger det noen kostnadsbomber i prosjektet? I sitt tilbudsbrev opplyser Ergo om at tilbudsdokumentene lastet opp til KRDs Sharepoint-server kunne åpnes med passordet «ittinget2010» (http://bit.ly/4DsM0t). Skal vi virkelig legge demokratiet i hendene til en leverandør som bryter de mest basale retningslinjer for trygge passord?

Hans Ekkehard Plesser,
førsteamanuensis i informatikk ved Universitetet for miljø- og biovitenskap
hans.ekkehard.plesser@umb.no