Er elektroniske valg trygge?

Kai A. Olsen, professor i informatikk, Høgskolen i Molde og Universitetet i Bergen

Ålesund er i år med i en forsøksordning der en kan stemme fra egen PC, over Internett. Motivet for en slik form for stemmegivning er at det vil bli lettere å delta når en ikke må møte opp i et valglokale. Vi gjør jo mye annet på Internett, så hvorfor ikke også kunne stemme her? Imidlertid har andre kommuner i Norge, som Oslo, sagt nei til å være med på forsøksordningen, med den begrunnelse at de ikke stoler på et elektronisk system.

Nå vil stemmegivning på Internett bryte med en viktig regel ved ethvert demokratisk valg, det at stemmegivningen skal skje i et godkjent valglokale der ingen kan se hva du stemmer. Organisasjonen for sikkerhet og samarbeid i Europa (OSSE) har dette som et klart krav i sin håndbok for demokratiske valg. Spesielt kan en være redd for at patriarker i enkelte innvandrerfamilier vil stemme for alle familiens medlemmer. Reza Rezaee, bystyremedlem i Oslo, med bakgrunn fra Irak nevner dette som en aktuell problemstilling. Men vi skal heller ikke se bort fra at det nå blir mulig å selge stemmer. I Kommunaldepartementet viser en til at dette løses ved at en kan angre seg, å stemme flere ganger. Men hva om en gir fra seg PIN-kodene? Da vil patriarken eller den som har kjøpt stemmen ha full kontroll, om da ikke den stemmeberettige selv møter opp i valglokalet på valgdagen. Patriarken kan nok kontrollere hvor familiemedlemmene er på denne dagen, mens en slik situasjon kun vil være en marginal risiko for den som har kjøpt en stemme.

Nå garanterer Kommunaldepartementet at systemet er sikkert, mot hacking, mot at stemmen kan bli endret eller mot at noen kan få vite hva du har stemt. Dette skal gjelde selv om maskinen din har et virus. Vi skal ta dette med en klype salt. I de siste årene har hackere brutt seg inn i mange ”sikre” systemer. Nå var det kanskje ikke så vanskelig å hacke seg inn i fylkeskommunale systemer, eller systemene til politiet, men hos Sony var det nok en utfordring. Likevel fikk hackerne adgang til konfidensielle data for millioner av brukere av Sony’s spillprogrammer. Også kredittkortselskap, den amerikanske etterretnings-organisasjonen CIA og sikkerhetsselskaper er blitt rammet. Mange husker DVD-Jon, vår norske hacker, som knekte kopieringskoden på DVD. Det vi altså ser er at tilsynelatende sikre systemer kan knekkes.

Mens det e-valg systemet vi bruker i Norge utvilsomt er vanskelig å hacke, er det derfor likevel sterkt å garantere at det er sikkert. En mulig svakhet i systemet kan for eksempel være i det øyeblikket stemmen blir avgitt. Et virus på PC’en vil kunne se hva brukeren gjør. Det kan gjøres før krypteringen, altså før kodingen av resultatet blir utført. I verste fall kan viruset generere en side som ligner på den ekte, for så å endre stemmegivningen. Det vil kreve ressurser å få dette til i stor målestokk, og det er lite trolig at politiske partier vil stå bak slik valgfusk. Men politiske avgjørelser, alt fra å selge aksjer til å bygge veier, kan gjelde store pengebeløp. Derfor kan andre aktører ha interesse av å påvirke valgresultatet.

Det som er mest betenkelig er imidlertid at disse tekniske systemene blir så kompliserte at en må være dataekspert og ha tilgang til hele systemet for å avgjøre om det er sikkert. Det paradoksale er at om en skulle gi slik tilgang så vil det kunne brukes til å svekke sikkerheten. Altså vil ethvert elektronisk system forutsette at vi stoler på dem som har laget systemet. Både med hensyn på at de har god nok kompetanse til å bygge et sikkert system, og at de ikke har egne motiver for å fikse resultatene. Dagens system, med stemmesedler, konvolutter og urner kan virke primitivt i en datatid. Det har imidlertid den store fordelen at hver og en av oss kan vurdere om det er sikkert.