

Vår saksbehandler
Avdelingsdirektør Christophe Birkeland
Senioringeniør Lars Borgos

Vår dato
2006-09-29
Tidligere dato
2006-03-13

Vår referanse
2006/00597-002/NSM/008
Tidligere referanse
06/532-1 MAR



Til
Kommunal- og regionaldepartementet

Kopi til

Internt

Intern kopi

Høring - Rapport H-2185 om "Elektronisk stemmegivning - utfordringer og muligheter"

Det vises til Deres høringsbrev av 13. mars 2006 om saken.

NSM støtter hovedanbefalingene som er gitt i rapporten. Vi vil knytte følgende merknader til rapporten.

Generelt:

Elektronisk stemmegivning uten papirbaserte backup – løsninger bør ikke innføres før det er etablert erfaring både nasjonalt og internasjonalt med elektroniske valgløsninger som har bevist sin robusthet. NSM deler derfor synet med at en elektronisk løsning bør innføres trinnvis.

Våre merknader er i det vesentligste konsentrert om de forhold som berøres i rapportens kapittel 8 "Tekniske utfordringer og mulige løsninger".

Systemets tilgjengelighet:

I rapporten er det lagt stor vekt på, og foretatt en grundig utredning av, forhold knyttet til elektronisk valgsystems integritet. NSM har ingen merknader til de vurderinger som er gjort i denne sammenheng. Med hensyn til konfidensialitetsvurderingene (anonym stemmegivning) synes også de vurderinger som er gjort gode. Vi vil imidlertid påpeke at utfordringene knyttet til tilgjengelighet, som den tredje pilaren i et helhetlig sikkerhetskonsept, er store. Dette gjelder spesielt i forhold til stemmegivning i ukontrollerte omgivelser (utenfor valglokalet), og særlig med internettbaserte løsninger. Sikker beskyttelse mot tjenestenektangrep kan ikke garanteres med dagens teknologi. På side 93 i rapporten uttales at flere stemmemottakstjenere vil vanskeliggjøre et tjenestenektangrep. Dette er for så vidt riktig, men det er likevel ikke praktisk mulig å sikre seg mot denne trusselen. Selv et relativt stort antall servere vil være et enkelt mål for en målbevisst aktør.

Vår dato

Vår referanse

2006/00597-002/NSM/008

Elektroniske løsninger i ukontrollerte omgivelser:

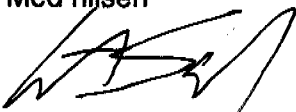
På side 94 omtales en løsning med personlig datamaskin med spesialoperativsystem. Her uttales at stemmegivning med oppstart fra CD-rom i prinsippet blir like sikkert som elektronisk stemmegivning i kontrollerte omgivelser. NSM vil påpeke at undergrunnsmiljøer arbeider aktivt for å utvikle ondsinnet programvare som infiserer BIOS. Dersom denne angrepsmetoden lykkes betyr det at selv ved oppstart av maskin fra dedikert CD-rom kan man risikere at spion – programmer likevel er aktive.

Sertifisering:

Det synes fornuftig å legge opp til en trinnvis utprøving av elektroniske valgløsninger. Den tekniske kravspesifikasjonen kan, slik som også påpekt i Ministerrådets rekommendasjon, utformes ved hjelp av standarden Common Criteria (CC) eller ISO 15408 i form av en såkalt "Protection Profile (PP)". NSM støtter denne tilnærmingen og anbefaler i tillegg evaluering og eventuelt sertifisering av PP før myndighetene benytter denne i samband med anskaffelse av valgløsninger, herunder også i samband med forsøksvirksomheten. Dette for å sikre at kravspesifikasjonen er tilstrekkelig gjennomarbeidet og ikke inneholder vesentlige svakheter som kan forringe og forsinke forsøksvirksomheten. Bakgrunnen for anbefalingen er også at CC også er et anvendelig verktøy for å sikre god produktutvikling og dokumentasjon med tanke på senere sertifisering av produktet. Det ligger i dette at selve utviklings- og sertifiseringsprosessen samlet blir mer effektiv og mindre kostnadskreven for industrien og sertifiseringsmyndigheten.

NSM er noe usikre på hva som ligger i terminologien "kritiske deler av løsningen...", jf 2.6 i rapporten, men antar dette spørsmålet blir håndtert nærmere i forsøksperioden. Det er grunn til å peke på at sertifisering etter CC kan gjennomføres på ulike tillitsnivåer, der dybde og omfang av undersøkelsene øker desto høyere tillitsnivå som ligger til grunn. Det kan dermed legges til rette for at enkelte deler av løsningen med høye sikkerhetskrav kan inneholde komponenter med et høyt tillitsnivå, mens øvrige deler av løsningen kan inneholde komponenter med et lavere tillitsnivå. Dette med bakgrunn i at et sertifisert produkt gjennomgående er mer velprøvd, bedre dokumentert og mer tillitvekkende enn et ikke-sertifisert produkt. NSM mener derfor det utelukkende bør anvendes sertifiserte produkter i en valgløsning, men at en bør se nærmere på hvilket tillitsnivå som er nødvendig i de enkelte delene av løsningen.

Med hilsen



Geir Samuelson
Assisterende direktør